

de Correspondent

MAURITS MARTIJN +
DIMITRI TOKMETZIS

JE HEBT WÉL IETS TE VERBERGEN

OVER HET LEVENSBELANG VAN PRIVACY

'Ik dacht echt dat ik veel wist van alle privacyproblematiek, maar ik heb dit fabelachtige boek met open mond gelezen. Nog nooit werd de discussie rondom privacy zo toegankelijk uitgelegd. Het is van absolute wereldklasse.'
– ALEXANDER KLÖPPING

'Martijn en Tokmetzis laten het belang van privacy treffend zien.'
– *de Volkskrant* ****

'In *Je hebt wél iets te verbergen* leggen Maurits Martijn en Dimitri Tokmetzis al hun grondig verworven inzichten voor ons bloot. Dit noodzakelijke boek is een noodklok en strijdershandboek in één, vloeiend en meeslepend, informatief en mobiliserend geschreven. Wat je nooit wist dat je moest weten, of waarvan je al wel een vermoeden had, wordt nu bevestigd: we hebben van alles te verbergen, maar zijn nog nooit zo naakt geweest.

Martijn en Tokmetzis schilderen een wervelend dystopia van dataspaghetti, techno-optimisme, Kafka in de polder, datahonger, surveillancekapitalisme, aangestuurd door moederschip Google. Is er nog tijd om er iets aan te doen? Ja, maar er is wel een omwenteling nodig, hopelijk mede aangezwengeld door dit boek.'
– BEATRICE DE GRAAF, hoogleraar Internationale Betrekkingen aan de Universiteit Utrecht

'Maurits Martijn en Dimitri Tokmetzis behoren tot de meest toonaangevende journalisten op het gebied van de schaduwzijdes van de digitaliserende samenleving.'
– ANCILLA VAN DE LEEST, lijsttrekker Piratenpartij

‘Privacy is voor veel journalisten een ingewikkeld onderwerp. Maurits Martijn en Dimitri Tokmetzis hebben daar bij *De Correspondent* geen last van. Met hun diepgravende onderzoeksjournalistiek leggen ze feilloos de pijnpunten in onze digitale samenleving bloot en laten ze zien dat technologie ook altijd een politieke dimensie heeft.’
– HANS DE ZWART, directeur Bits of Freedom

‘Dit verhaal moet iedereen lezen die de machtsverhoudingen in onze huidige gedigitaliseerde samenleving wil begrijpen. Wat op het spel staat is geen individuele zorg van een paar privacyvoorvechters, maar een zaak die ons allemaal aangaat: we worden online gemanipuleerd zonder dat we mogen weten hoe.’
– BART JACOBS, hoogleraar Computerbeveiliging aan de Radboud Universiteit Nijmegen

Eerste druk september 2016
Tweede druk september 2016
Omslagontwerp door Harald Dunnink (Momkai) en Leon Postma (*De Correspondent*)
Illustratie auteurs Cléa Dieudonné
Redactie Harminke Medendorp
Eindredactie Andreas Jonkers
Correctie Annelieke Tillema
Vormgeving binnenwerk Pre Press Media Groep
Druk Koninklijke Wöhrmann, Zutphen
ISBN 9789082520330
NUR 320

Deze publicatie is tot stand gekomen met steun van het Fonds Bijzondere Journalistieke Projecten.

FONDS Bijzondere JOURNALISTIEKE PROJECTEN

www.fondsbjp.nl

MAURITS MARTIJN +
DIMITRI TOKMETZIS

JE HEBT WÉL IETS TE VERBERGEN

OVER HET LEVENSBELANG VAN PRIVACY

de Correspondent

2016

Inhoud

Inleiding: Ik heb niets te verbergen 11

1 Smartphones en andere zwarte dozen 21
Hoe ons privacybegrip hopeloos is verouderd

2 Hackers en de NSA 47
Waarom ieders persoonlijke gegevens fundamentele risico's lopen

3 Google en de Belastingdienst 71
Hoe de grote datagraaiers onze gegevens in hun greep hebben

4 Surveillancekapitalisten en sturende overheden 113
Waarom de jacht op onze gedragsgegevens definitief is geopend

5 Autonomie en democratie 139
Waarom privacy over veel meer gaat dan persoonsgegevens

Conclusie: Tijd voor tegenmacht 181
Epiloog: Een nieuw privacyklimaat 197
Zo kun je jezelf (en je omgeving) beschermen 207

Dankwoord 209
Verantwoording 211
Bronnen 213

'Privacy niet belangrijk vinden omdat je niets te verbergen hebt, is hetzelfde als niet geven om vrijheid van meningsuiting omdat je niets te zeggen hebt.'[1]

— EDWARD SNOWDEN

'Als je iets doet waarvan je niet wilt dat anderen het weten, kun je het beter misschien maar helemaal niet doen.'[2]

— BESTUURSVOORZITTER VAN ALPHABET (GOOGLE) ERIC SCHMIDT

Inleiding

Ik heb niets te verbergen

Op een ochtend in 1977 tuurt Chris van der Ziel naar zijn huis in de Cornelis Houtmanstraat in Delfzijl. Dat dak, daar is iets mee. Hij loopt naar binnen, gaat de trap op en bekijkt het plafond in de slaapkamer. Er zit een duidelijke knik in, tussen de zolder en het dak móét iets zijn.

Met zijn vrouw begint hij het plafond te slopen. Het behang eraf, het pleisterwerk open, de isolatie los. Dan: een harde kraak. Het hele dakbeschot stort in. Gruis en planken komen naar beneden, samen met de verklaring voor het mysterie van de plafondknik: een stapel dikke boeken.

Van der Ziel en zijn vrouw slaan ze open en vinden een gedetailleerde verslaglegging uit een stoffig verleden. Boekhoudingen, notities van bijeenkomsten, persoonlijke brieven. De aantekeningen stammen van vlak voor de Tweede Wereldoorlog. Het blijken documenten van de Joodse gemeenschap van Delfzijl. Elk Joods gezin staat met naam, adres en familieverbanden vermeld.

Later zal de familie Van der Ziel ontdekken dat een eerdere bewoner van het huis aan de Cornelis Houtmanstraat een rabbijn was. Na het uitbreken van de oorlog in 1940 verstopte hij de boekhouding onder het dak. Als de Duitse bezetter de administratie in handen had gekregen, had die alle benodigde informatie om iedere Jood in de gemeente Delfzijl op te pakken. De rabbijn wilde zijn gemeenschap beschermen.[3]

We maken ons zorgen

Zeker sinds de onthullingen van Edward Snowden in juni 2013 over de datazucht van de Amerikaanse National Security Agency (NSA) is er gigantisch veel aandacht voor privacy. Boeken over privacy en surveillance, het in de gaten houden van groepen mensen, zijn bestsellers. Onderzoeksjournalistiek over de verzameldrift van overheden en bedrijven krijgt hoge journalistieke onderscheidingen. En *Citizenfour*, de film over Edward Snowden, werd in 2015 bekroond met een Oscar voor beste documentaire.

In opiniepeilingen geeft steeds een grote meerderheid aan haar privacy zeer belangrijk te vinden. Van de deelnemers aan een onderzoek onder 28.000 Europese burgers in 2015 had slechts 15 procent het gevoel controle te hebben over zijn persoonlijke data. 70 procent van de ondervraagden was bang dat zijn gegevens voor andere doeleinden worden gebruikt dan waarvoor ze verzameld worden.[4] En in een recente poll onder 24.143 internetgebruikers uit 24 landen geeft 79 procent van de ondervraagden aan zich zorgen te maken over het gebrek aan online privacy.[5]

Als we kijken naar ons gedrag, doemt een ander beeld op. Dan vinden we privacy opeens veel minder belangrijk dan we de opiniepeilers vertellen. Dan geeft 45 procent van de Nederlanders aan bereid te zijn gezondheidsdata af te staan in ruil voor premiekorting.[6] Dan gebruiken we Google en Facebook nog steeds dat het een lieve lust is. Dan verdiepen we ons totaal niet in privacyvoorwaarden en klikken we klakkeloos op 'ja, ik heb de voorwaarden gelezen' en 'ja, ik ga akkoord.' Dan stemmen we gewoon weer op politieke partijen voor wie privacy het afvoerputje van hun partijprogramma is.

Privacy is een waarde die het heel snel van andere waarden verliest. Als we de keuze hebben tussen privacy en veiligheid, of tussen privacy en gemak, of tussen privacy en minder betalen, dan kiezen we meestal niet voor privacy. Je kunt stellen dat privacy aan hetzelfde euvel lijdt als het klimaat: het baart ons grote zorgen, zeggen we, om vervolgens stilletjes op dezelfde voet verder te gaan en voor de makkelijkste weg te kiezen – zoals we ook massaal olieslurpende auto's blijven rijden en het vliegtuig nemen naar onze vakantiebestemming.

We hebben niets te verbergen

Er zijn vijf woorden die de essentie van onze paradoxale houding samenvatten. Een zinnetje dat symboliseert dat we privacy geen echte prioriteit geven:

'Ik heb niets te verbergen.'

In discussies over privacy vallen deze vijf woorden steevast. En anders wel in een van deze varianten:

'Ik doe niets illegaals' of 'Ik doe niets fout of verkeerd.' Meestal gevolgd door een van deze toevoegingen:
- 'Ik heb niets te verbergen, *dus ik heb niets te vrezen.'*
- 'Ik heb niets te verbergen, *want ik ben geen terrorist, crimineel of pedofiel.'*
- 'Ik heb niets te verbergen, *dus de NSA, de AIVD, de Belastingdienst, Google en Facebook mogen alles van mij weten.'*

Wij, twee journalisten die over privacy en surveillance schrijven, krijgen deze vijf woorden al jaren te horen. We hebben er tot onze frustratie maar matig antwoord op. Privacy is te belangrijk om af te doen als iets wat alleen criminelen, terroristen of pedofielen nodig hebben. Privacy is van levensbelang, het is de smeerolie van een gezonde democratie en een voorwaarde voor een functionerende rechtsstaat. Maar ja, bewijs dat maar eens.

Wij hebben in de loop der tijd heel wat tegenwerpingen uitgeprobeerd. Als iemand zegt 'ik heb niets te verbergen,' dan antwoor-

den we soms: 'Oké, trek dan je kleren maar uit.' Als we in een wijsneuzeriger bui zijn, citeren we graag Edward Snowden: 'Privacy niet belangrijk vinden omdat je niets te verbergen hebt, is hetzelfde als niet geven om vrijheid van meningsuiting omdat je niets te zeggen hebt.' En soms halen we scheurkalenderfilosofe Loesje aan: 'Ik heb niets te verbergen. Maar dat hoeven ze niet te weten.'

Maar met spitsvondigheden alleen red je het niet. Het 'ik heb niets te verbergen'-argument is hardnekkig. Politici en CEO's gebruiken het als moreel appèl als zij worden aangesproken op de wijze waarop zij met onze gegevens omgaan. Zoals Eric Schmidt, de bestuursvoorzitter van Google, die in een interview zei: 'Als je iets doet waarvan je niet wilt dat anderen het weten, kun je het beter misschien maar helemaal niet doen.' Of de Belgische minister Jambon, die na de aanslagen in Brussel in het voorjaar van 2016 een centrale database met vingerafdrukken van iedere Belg voorstelde: 'Maar mensen die niets te verbergen hebben, moeten toch geen schrik hebben dat je hun vingerafdruk neemt?'

We zien het niet

Voordat wij drie jaar geleden bij online journalistiek platform *De Correspondent* aan de slag gingen, schreven we al een aantal jaar voor andere media over privacy en surveillance. Dat was in het pre-Snowdentijdperk, de tijd dat je als journalist nog je uiterste best moest doen om een hoofdredacteur ervan te overtuigen dat een verhaal over privacy de moeite waard was.

We stuitten vaak op glazige blikken bij onze bazen. Maar dat lag ook – of misschien wel vooral – aan onszelf. We konden het simpelweg niet goed uitleggen. Ja, bedrijven die ons surfgedrag bijhouden zijn griezelig, maar waarom precies? Ja, de risicoprofielen die overheden van ons maken zijn totaal ondoorzichtig, maar die kunnen toch ook heel nuttig zijn? Ja, Google en Facebook kennen ons beter dan onze beste vrienden, maar wat is daar eigenlijk mis mee? Zonder privacy geen democratie, zeiden we, maar hoe zit dat dan? En waarom is 'ik heb niets te verbergen, dus ook niets te vrezen' zo'n naïef argument? Wat hebben we dan wél te verbergen?

Een belangrijke reden dat deze vragen zo verdomd moeilijk zijn te beantwoorden, is dat we niet zien wat er met onze gegevens gebeurt. We zien niet welke overheden, bedrijven en criminelen op onze data jagen, hoe ze dat doen, waarom ze het doen, wat ze er uiteindelijk mee doen en hoe dit onze levens beïnvloedt.

Deze onzichtbaarheid verklaart ook onze onverschilligheid. Althans: ons gebrek aan daadkracht. Ze verklaart waarom wij het belang van privacy vooral met de mond belijden. Het verklaart waarom wij denken niets te verbergen te hebben.

We zien het niet en daardoor begrijpen we het niet en daardoor voelen we de urgentie niet. Zoals er een ernstige dijkdoorbraak moet komen voordat we de risico's van klimaatverandering onder ogen zien, zo moet er eerst iets goed misgaan voordat we het belang van privacy tot ons laten doordringen.

Precies daarom openen wij dit boek met het verhaal over het plafond van Chris van der Ziel. Want die Joodse gezinnen in Delfzijl dachten ook niets te verbergen te hebben. Totdat in 1940 de Duitse bezetter kwam en de onschuldige informatie uit de boeken in één klap dodelijk werd.

Hoe maken wij het onzichtbare zichtbaar?

Toen wij drie jaar geleden besloten samen op te trekken in ons journalistieke onderzoek, realiseerden wij ons dat dit de sleutel kon zijn: als wij erin zouden slagen om het onzichtbare zichtbaar te maken, dan konden we het belang van privacy laten zien en tastbare argumenten aanvoeren tegen 'ik heb niets te verbergen.'

Dit boek is het resultaat van die driejarige zoektocht.

Goed onderzoek begint bij een scherpe definitie van het onderwerp. Dat is met privacy geen eenvoudige opgave. Over de vele vormen en betekenissen van privacy zijn bibliotheken volgeschreven. Er bestaat bijvoorbeeld zoiets als 'fysieke' privacy, het idee dat mensen jou niet mogen aanraken als je daar geen zin in hebt. Er is 'ruimtelijke' privacy, dat gaat over iemands huis als de plek waarvan onbevoegden niet horen te weten wat er gebeurt. Er is ook 'relationele' privacy, waarbij het draait om vertrouwen binnen verschillende relaties.[7]

In dit boek staat privacy als de bescherming van persoonlijke informatie centraal, 'informationele' privacy volgens de literatuur. Onze opvatting van persoonlijke informatie – of 'data' en 'gegevens' – is breed. Van telefoonnummer tot e-mailadres, van online zoekgedrag tot burgerservicenummer, van huisadres tot IP-adres.

Wij zullen twee sporen volgen. Allereerst onderzoeken wij wat er dagelijks met onze persoonlijke informatie gebeurt. Tegelijkertijd zoeken wij naar het belang van privacy. Waarom moeten wij ons hier zorgen over maken?

De methode die wij daarbij hanteren, is enerzijds klassiek journalistiek: we beantwoorden de wie-, wat-, waar-, waarom-, hoe-vragen over persoonlijke data. Anderzijds maken we gebruik van nieuwe journalistieke onderzoeksmethodes. In de onderzoeksjournalistiek geldt dat je, als je het naadje van de kous wilt weten, het geldspoor moet volgen: *follow the money*. Als je het geld volgt, stuit je op belangen en macht en leg je bloot wat onder de oppervlakte ligt. Voor onze zoektocht houden wij vast aan een ander adagium: *follow the data*. Door datasporen te volgen, kunnen we laten zien wat voor informatie wij allemaal over onszelf weggeven en hoe tientallen bedrijven en instanties die data onderling verhandelen en delen. Zo kunnen wij uitvinden welke beslissingen er worden genomen op basis van die data en aantonen hoe die beslissingen onze levens bepalen.

Onze zoektocht brengt ons van de dataslurpende Bijenkorfapp naar de achterdeuren van de Belastingdienst, en van zwarte

markten in de krochten van het internet tot aan de Amerikaanse douane. We hebben smartphones gekraakt, wifinetwerken gehackt, internetverkeer onderschept, sociale media ontleed, databases leeggetrokken, hackbijeenkomsten gehouden, honderden privacyvoorwaarden uitgekamd, tientallen openbaarheidsverzoeken ingediend en honderden deskundigen en denkers in binnen- en buitenland gesproken.

We kunnen alvast verklappen: je hebt wél iets te verbergen.

'Als een machine efficiënt loopt [...] dan hoeft men zich alleen te richten op de input en de output, en niet op zijn interne complexiteit. Dus, paradoxaal genoeg, hoe meer succes wetenschap en technologie boeken, hoe intransparanter en obscuurder ze worden.'[8]

— FILOSOOF BRUNO LATOUR

'Als een onbekende man je vraagt je kleren uit te trekken, denk je dat hij gek is; als de onbekende man een dokter is, zou het gepast zijn; als het iemand is met wie je voor het eerst datet, zou het bruusk zijn; op een tweede of derde date is dat misschien wél gewenst.'[9]

— PRIVACYEXPERTS OMER TENE EN JULES POLONETSKY

1

Smartphones en andere zwarte dozen

Hoe ons privacybegrip hopeloos is verouderd

Wij beginnen onze zoektocht naar het belang van privacy in juli 2013 met het credo: beter goed gejat dan slecht bedacht. In de geweldige verhalenreeks 'What They Know' onderzocht een team van onderzoeksjournalisten en technisch experts van *The Wall Street Journal* de verborgen economie achter het internet.[10] Gedurende twee jaar onthulde de kwaliteitskrant hoe de Amerikaanse internetgebruiker al surfend continu wordt bespied door honderden – vaak onbekende – bedrijven. De journalisten slaagden erin een internationale marktplaats bloot te leggen waar onze persoonlijke gegevens en datastromen handelswaar zijn zonder dat wij het zien.

Wij willen nagaan of we op Nederlandse sites net zoveel door bedrijven bespioneerd worden als in de Verenigde Staten. Alleen: hoe onderzoek je dit? Voor ons is dit nieuw terrein, ook al gaan wij beiden zeker niet bleu dit onderwerp in. Dimitri publiceerde in 2012 al uitvoerig over privacy en digitale profielen in zijn boek *De digitale schaduw*. Maurits schreef een aantal jaar voor *Vrij Nederland* over hackerscultuur, de surveillance-industrie en de datahonger van de Nederlandse overheid. Maar dit is andere koek.

Dit is een nieuwe, opwindende vorm van onderzoeksjournalistiek.

De journalisten van *The Wall Street Journal* werkten intensief samen met techneuten en onderzoekers. Het team bouwde zelf software om het web af te kunnen struinen en combineerde klassieke vormen van journalistiek met baanbrekende datajournalistiek. De serie werd geprezen en genomineerd voor een Pulitzerprijs.

Via via komen we in contact met Ashkan Soltani, de hoofdonderzoeker van 'What They Know.' In een Amsterdamse koffietent legt hij ons uit hoe we ons onderzoek op kunnen zetten. 'Journalistiek zal in toenemende mate dit soort onderzoek nodig hebben,' vertelt hij. Soltani raadt ons aan te beginnen bij de websites die we allen dagelijks bezoeken op onze desk- of laptop. Helaas kan hij ons daar niet bij helpen, zegt hij. Niet veel later begrijpen wij waarom: hij is ingehuurd door *The Washington Post* om de technische analyse te doen van de honderden documenten die via Edward Snowden zijn uitgelekt. De krant en Soltani zullen voor hun berichtgeving dit keer wel bekroond worden met een Pulitzerprijs.

De gluurders op onze laptops

Op advies van Soltani schakelen we de hulp in van wetenschappers die ervaring hebben met dit soort onderzoek: Lonneke van der Velden en Anne Helmond van de Universiteit van Amsterdam. Beiden zijn betrokken bij het Digital Methods Initiative van de universiteit, waar zij met collega's de zogenoemde Tracker Tracker-tool ontwikkelden.[11] Deze software kan voor een belangrijk deel hetzelfde als de software van de onderzoekers van *The Wall Street Journal*. Met de tool is het mogelijk om een site te scannen en zo de zogenoemde *trackers* op de site te identificeren en in kaart te brengen.

Trackers worden door bedrijven ingezet om informatie over websitebezoekers te verzamelen. Meestal zijn dit cookies: data die op jouw computer of laptop worden achtergelaten als je een site bezoekt. Daarmee kunnen bedrijven je surfgedrag, locatie en informatie over je computer aan elkaar koppelen om daarmee een persoonlijk dossier op te bouwen. Vaak wordt meer geavanceerde technologie ingezet. Dan registreren bedrijven bijvoorbeeld de instellingen van je browser: de taal, welke plug-ins je hebt geïnstalleerd, het besturingssysteem. Soms werken trackers ook met geluid. Er bestaan apps op smart-tv's die een voor ons onhoorbare toon versturen die wordt opgevangen door een app op je telefoon.[12] Zo is te achterhalen naar welke programma's je kijkt en welke apparaten er bij elkaar in de buurt zijn.[13]

Bedrijven trekken alles uit de kast om online zo veel mogelijk over ons te weten te komen. Want hoe meer zij weten, hoe beter en effectiever zij ons online advertenties kunnen voorschotelen. Dit gaat over miljarden. In 2015 werd er wereldwijd voor het eerst meer aan webadvertenties besteed dan aan tv-reclames: zo'n 125 miljard euro.[14]

Met de Tracker Tracker-tool van de Universiteit van Amsterdam is het mogelijk om te achterhalen welke trackers websites achterlaten op de computers van bezoekers. We gaan aan de slag en nemen op onze laptop de honderd populairste sites van Nederland onder de loep: van nu.nl tot marktplaats.nl en van zalando.nl tot voetbalzone.nl. En plotseling ziet het internet er onherkenbaar uit. Aan de voorkant doet het zich voor als een verzameling sites, geklets op sociale media, kattenfilmpjes en links, aan de achterkant zien we met de tool een verzameling commerciële partijen die aan elkaar vastgeklonterd zitten rond onze datastromen.

In totaal ontdekken we op de honderd geteste sites trackers van 215 verschillende bedrijven. We besluiten de privacyvoorwaarden van deze bedrijven door te vlooien: welke data verzamelen ze, hoelang bewaren ze die en met wie delen ze die?

We schrikken van de resultaten. Neem nieuwssite nu.nl. In totaal vinden we 44 trackers op die site, onder meer van bedrijven die in hun voorwaarden schrijven dat zij de recente surfgeschiedenis en ingevoerde zoektermen van jou als sitebezoeker verzamelen, je type computer registreren en je demografische gegevens achterhalen. Twee bedrijven zeggen in hun privacyvoorwaarden daar 'persoonlijk identificerende informatie' aan te kunnen koppelen die zij van andere partijen kopen of ontvangen, zoals je

naam en geboortedatum, je financiële situatie en informatie over je werkgever.

Als we surfen en browsen zijn we geneigd ons alleen en onbespied te wanen, zoals we ons alleen en onbespied wanen als we 's ochtends de krant lezen aan de keukentafel. Maar online worden we constant gestalkt door onbekende partijen die van alles van ons willen weten. Ze begluren en analyseren ons. Zij zien ons, we zien hen niet.

De gluurders op onze smartphones

Na de huis-tuin-en-keukenlaptop vervolgen we ons onderzoek met het apparaat dat we de hele dag door gebruiken: de smartphone. De smartphone is zonder enige twijfel de succesvolste consumententechnologie van de afgelopen tien jaar. Er zijn nu meer dan 2 miljard gebruikers en dat aantal stijgt rap. We gebruiken de smartphone ook steeds méér: meer minuten per dag, meer dataverbruik.[15]

Tegelijkertijd begrijpen we nagenoeg niks van dat ding.

Het is een ultiem voorbeeld van wat de Franse filosoof Bruno Latour een 'black box' noemt: een apparaat dat werkt als een trein maar waarvan de échte werking mysterieus blijft. 'Als een machine efficiënt loopt,' schrijft Latour, 'dan hoeft men zich alleen te richten op de input en de output, en niet op zijn interne complexiteit.'

Ja, je weet waar je op moet drukken om de smartphone te gebruiken (input) en begrijpt *wat* hij als reactie daarop zal doen (output) – bellen, surfen, appen, et cetera – maar *hoe* het apparaat dat allemaal doet? Niet voor niets luidde de slogan van Apple jarenlang: '*It just works.*'

Bij de smartphone is het een bewuste keus geweest om 'm dicht te houden. In principe is een smartphone een computer, met dit verschil: een normale computer is relatief open. Je kunt er zelf

programma's voor schrijven en erop installeren wat je wilt. Toen Steve Jobs in 2007 de iPhone lanceerde, maakte hij direct duidelijk dat dit niet voor zijn kroonjuweel zou gelden. 'Wij bepalen wat op de telefoon wordt toegelaten,' zei Jobs tijdens de presentatie van het apparaat. Een aanpak die de standaard zou worden in de booming smartphonebusiness. Want je kunt swipen wat je wilt, nergens zul je zien wat het besturingssysteem precies doet en welke data jouw apps gebruiken.

En dat is raar. Want als je nagaat welke rol de smartphone in ons leven speelt, dan kun je eenvoudig beargumenteren dat wij het ding juist wél zouden moeten doorgronden. De smartphone is – nog meer dan onze laptop – ons venster op de wereld, ons primaire communicatiemiddel, onze assistent.

Wie toch onder die motorkap wil kijken, heeft geen andere keus dan zijn eigen smartphone te hacken; die motorkap open te breken met een digitale koevoet. De terminologie om het apparaat binnen te kunnen dringen is wat dat betreft veelzeggend. Als je meer te zeggen wilt hebben over een iPhone, moet je hem 'jailbreaken.' Op een Androidtoestel moet je '*root access*' zien te krijgen. In de computerwereld is degene met root access de beheerder. De boodschap is duidelijk: jij bent dat niet.

Ashkan Soltani van *The Wall Street Journal* heeft ons gewaarschuwd dat het blootleggen van trackers op een desk- of laptop kinderspel is vergeleken met het doorgronden van de datastromen van een smartphone. De Tracker Tracker-tool die wij gebruikten voor ons onderzoek naar de datastromen op de laptop was al ontwikkeld, en was bovendien vrij simpel te gebruiken. Een smartphone hacken vergt meer precisiewerk. Toch gaan we de uitdaging aan.

En dus ligt er op een zekere dag in 2014 voor ons op tafel een Samsung Galaxy Note III, een smartphone die draait op Android, het besturingssysteem van Google. Op een iPhone moeten adverteerders per app toestemming vragen of ze bij je contact- of locatie-

gegevens mogen. Op een Androidsysteem geef je die toestemming voordat je de app installeert: je moet alle voorwaarden accepteren, anders kun je de app niet gebruiken.[16]

We besluiten de populaire winkelapp van de Bijenkorf op trackers te testen. Voordat de installatie van start gaat, vraagt Googles appwinkel of we de app voor een aantal zaken toestemming willen verlenen. Normaal gesproken doen we dat gedachteloos, nu besluiten we er eens goed voor te gaan zitten en zien we dat de app:

- Wil kunnen zien of we op een wifinetwerk zitten.
- Gebruik wil kunnen maken van de trilfunctie op onze smartphone en wil kunnen voorkomen dat het toestel in slaap sukkelt.
- Gegevens op onze geheugenkaart wil kunnen schrijven of wijzigen.
- Gebruik wil kunnen maken van de camera en onze netwerkgebaseerde en gps-locatie wil kunnen achterhalen.
- Toestemming wil om onze agenda te kunnen lezen en te wijzigen.
- O ja: de app wil ook eigenhandig mails kunnen sturen aan mensen die in die agenda staan.

Natuurlijk. Gaat uw gang, beste Bijenkorf.

Nu de app is geïnstalleerd, willen we de informatiestromen vanuit de app in kaart brengen.

We spreken met appontwikkelaars en hackers om een goede methode te vinden. Uiteindelijk komen we uit bij Charles, een softwarepakket waarmee je het dataverkeer van en naar je smartphone kunt onderscheppen en analyseren. Het programma wordt door app- en webontwikkelaars gebruikt om datastromen te volgen, bijvoorbeeld om te kijken of er nog fouten in de code zitten. Het dataverkeer van onze smartphone gaat met Charles niet rechtstreeks via de router, maar via onze computer het internet op. Charles kan zo alle datapakketjes van en naar de app netjes ordenen zodat wij kunnen zien welke informatie waar naartoe gaat. Zo'n onderschepping noemen hackers een *man-in-the-middle attack*.

Omdat internetverkeer soms is versleuteld, installeert Charles bovendien een vals beveiligingscertificaat, waardoor de app denkt met een veilige partij te communiceren. Charles stelt ons zo in staat om milliseconde na milliseconde te volgen met welke servers onze Samsungsmartphone contact legt en welke data daarbij worden verzonden en ontvangen. Ook informatie die om veiligheidsredenen versleuteld is.

Het is 11.47 uur als het feest kan beginnen. We drukken op de Bijenkorfapp. Nog voordat de app opent en de inhoud wordt geladen, zien we dat Google een cookie plaatst zodat het bedrijf ons gebruik van de app kan volgen. Kort daarna zien we dat de Bijenkorfapp ons toestel een uniek identificatienummer geeft waarna ook de Bijenkorf ons kan herkennen en volgen.

We besluiten in de app een Bijenkorf Card aan te vragen om te kunnen shoppen. Om 11.48 uur maakt de app contact met een server in Seattle in Amerika. Die is van Amazon en wordt gehuurd door Intershop, een bedrijf dat de Bijenkorf helpt zijn appgebruikers te analyseren. Ook statistiekbedrijf Shop2market komt het toneel opgestormd om, net als Google Analytics en DoubleClick, ons gedrag *swipe* na *swipe* te volgen.

In Charles zien we zo tientallen domeinnamen (bijvoorbeeld: www.openx.com) en IP-adressen (unieke code, zoals 214.235.32.234 die hoort bij apparaten die aangesloten zijn op het internet) over het scherm rollen. Sommige adverteerders en analysebedrijven herkennen we aan hun domeinnamen, andere zoeken we via hun IP-adressen op in openbare databases. Verder zien we dat sommige adverteerders een unieke code meesturen die op onze smartphone wordt bewaard, die ziet er bijvoorbeeld zo uit: uid=23462435lsdfgsxAJfdap0342ad4adfjS. Zo'n unieke code kunnen zij later gebruiken om ons te herkennen als we andere apps gebruiken.

Zodra wij onze Bijenkorf Card binnen hebben, zijn we klaar om te shoppen. We besluiten op een luxe zwartlederen laptoptas (ruim 500 euro) te klikken. En dan gebeurt er iets geks. In Charles verschijnt een brij aan codes en als we die regel na regel analyseren, ontdekken we patronen. IP-nummers die terug blijven komen. Woordjes als 'bid=0.5.' Verder duikt de naam Samsung veelvuldig op ons beeldscherm op. Wat dit allemaal betekent? Terwijl we naar de tas kijken, wordt onze smartphone besprongen door zeker achttien onlineadvertentiebedrijven die allerlei data naar hun servers sturen, over wie wij zijn, waar we zitten, welke app en wat voor hardware we gebruiken. In één enkele seconde is contact gelegd met servers in de Verenigde Staten, Zweden, Duitsland, Ierland en Nederland, die behoren tot bedrijven die luisteren naar namen als Improve Digital, Admeta, Adtech, Metrigo, Burst Media, Yieldlab, Switch Concepts, AppNexus, Sociomantic, Adscale, Rubicon Project, OpenX, Smart Adserver en Casale Media.

Wat doen die onbekende bedrijven daar?

Wat deze gluurders precies doen, zien we als we een andere app analyseren: AntiVirus Security FREE, die al meer dan honderd miljoen keer is gedownload op Androidapparaten. Als we na installatie het antivirusprogramma openen en Charles laten meedraaien, zien we dat de app virussen tegenhoudt, maar voor andere binnendringers de deur juist wagenwijd openzet: de ene na de andere adverteerder stormt onze smartphone binnen.

De eerste tracker wordt geplaatst door Google Analytics. Daarna zien we ook diens grote advertentiebroer DoubleClick verschijnen. Vervolgens meldt advertentieplatform MoPub zich en wijst onze telefoon een aantal unieke identificatienummers toe. Met deze letter- en cijfersoep kan MoPub ons later op andere sites en apps opnieuw herkennen. Het bedrijf ziet dan bijvoorbeeld dat we ook gezondheidsapp MyFitnessPal gebruiken, de spelletjes *Clash of Clans* en *Hay Days* spelen en populaire muziekapps als Spotify en Shazam openen. In Charles zien we dat MoPub ook weet dat we ons in Nederland bevinden, op het mobiele netwerk van hollandsnieuwe zitten en een Samsung Galaxy Note III gebruiken.

Er melden zich nog meer partijen. Het lijkt wel alsof er op ons geboden wordt. Prijzen schieten heen en weer. We zien een bod van 0,50 dollar langskomen. Na nog wat onderling gepraat van de servers komt er een winnend bod uit van 0,65 dollar. Advertentiebedrijf MobFox lijkt de strijd gewonnen te hebben, want dat bedrijf mag een advertentie van 320 x 50 pixels groot leveren in de AntiVirus Security FREE-app op onze smartphone. En dit allemaal in de tijdspanne van een hartslag.

We leren dat wat wij in eerste instantie aanzagen voor een aanval van advertentiebedrijven, in werkelijkheid een volledig geautomatiseerde veiling is. *Realtime bidding* geheten. De bieders op die veiling zijn advertentiebedrijven en onze data de te veilen objecten. Realtime bidding is de laatste jaren in razend tempo opgekomen. Het doel is om zo effectief mogelijk te adverteren. Een advertentie moet de adverteerder geld opleveren: je moet klikken en kopen. Hoe beter de realtime adverteerder jou weet te doorgronden, hoe effectiever hij kan adverteren. Het voordeel zit dus in de data. Informatie over jou.

In de praktijk werkt dat zo. Stel, je opent de AntiVirus Security FREE-app, die neemt dan contact op met een zogenoemd *demand-side platform*, een technologiebedrijf dat namens aanbieders advertentieruimte veilt. Bij het aanbod stuurt een demand-side platform basale informatie mee over de gebruiker en over de plek waar de advertentie komt te staan.

Dan wordt 100 milliseconden lang gewacht. Zoveel tijd krijgen alle aangesloten adverteerders om uit hun eigen databases extra informatie over jou te halen en hun computers uit te laten rekenen of een advertentie lucratief zal zijn of niet. Waar bevind je je? Met welk apparaat surf je op dat moment? Op welke sites ben je eerder geweest de afgelopen week? Hoe goed pas je in de doelgroep van

de campagne? Heeft de adverteerder jou al eerder een advertentie laten zien en wanneer was dat? Op welke positie op de site heeft die toen geadverteerd? Wat is de ervaring met die positie op de site? Binnen enkele seconden word je van top tot teen geanalyseerd.

Dan mogen de adverteerders bieden. Als alle biedingen zijn verzameld, wint de adverteerder met het hoogste bod. Die mag de advertentie leveren en een cookie plaatsen op jouw smartphone. De volgende keer dat je AntiVirus Security FREE gebruikt, word je door een extra tracker gevolgd.

Ook onze kinderen worden begluurd

Je zou denken dat niet iedereen onder het vergrootglas van trackers en *realtime bidders* mag liggen. Kinderen bijvoorbeeld. In de Europese privacywet staat dat identificerende gegevens van personen onder de zestien niet verzameld mogen worden, of dat ouders daar eerst toestemming voor moeten geven. De gedachte hierachter is dat kinderen nog niet in staat zijn om afgewogen keuzes te maken en hun eigen belangen altijd te herkennen, laat staan die te beschermen (laten we er voor het gemak even van uitgaan dat dit voor volwassenen wél geldt).

Veel websites, apps en online advertentiebedrijven zeggen deze gevoeligheid te erkennen en beloven in hun privacyvoorwaarden geen data over kinderen te verzamelen of daar heel voorzichtig mee om te gaan.

Het blijken loze beloften. Op de 72 kinderwebsites en -apps die we met Charles testen, worden we door minstens 179 verschillende bedrijven gevolgd. Neem studio100.be, waar we leuke spelletjes met Maya de Bij, Wickie de Viking, Mega Mindy, Bumba en K3 kunnen spelen. In de drie minuten die we op Studio100 doorbrengen, vinden er vier flitsveilingen plaats waar enkele tientallen bedrijven aan meedoen.

De door ons onderschepte datapakketjes verraden bovendien dat niet alleen adverteerders onze data krijgen. Zo wordt ook de DemDex-database van Adobe aangeroepen. DemDex is, in de aanprijzende woorden van Adobe, 'een product dat online en offline informatie uit iedere mogelijke bron integreert [...] waarmee je snel je meest waardevolle klanten kunt herkennen en ze gericht kunt aanspreken om ze zo tot handelen aan te zetten.' Lees: een advertentie plaatsen waarop een kind kan klikken om iets te kopen. Een ander bedrijf dat meedoet in de flitsveiling is Acxiom, een Amerikaanse datahandelaar die online dossiers beheert van honderden miljoenen consumenten.

Studio100 ontkent aanvankelijk onze bevindingen. Pas nadat we onze data opsturen, geeft het bedrijf schoorvoetend toe dat het inderdaad kinderen volgt en hun data verzamelt en verkoopt. In zijn privacyvoorwaarden schuift studio100.be overigens alle verantwoordelijkheid resoluut af. 'Wij kunnen niet garanderen dat deze derden op een betrouwbare of veilige manier met persoonsgegevens omgaan. Wij raden je aan de privacy policy van deze websites en applicaties te lezen alvorens ervan gebruik te maken.' Voor een bezoek aan studio100.be zouden we dan 54 privacyvoorwaarden moeten uitpluizen. Iedere ouder weet: die tijd krijg je niet als je kind een spel wil spelen.

En weten de meer dan honderd miljoen ouders die voor hun kinderen het spel *Minion Rush* hebben geïnstalleerd op hun Androidtelefoon wat deze gratis app daar allemaal voor terugkrijgt? Namelijk welke Twitter-, Facebook- en Google-accounts aanwezig zijn op hun smartphone, wie hun contacten zijn, wat het serienummer van het apparaat is, hoe de netwerken heten waarmee ze met het internet verbonden zijn, waar ze zich bevinden, wie hun telefoonprovider is, wat hun klantnummer daar is en welke apps ze hebben geïnstalleerd?

Voor de duidelijkheid: sommige gegevens heeft de app daadwerkelijk nodig. Je wilt bijvoorbeeld niet dat grote updates je

databundel opsnoepen, maar dat er even wordt gewacht met downloaden tot je op een wifinetwerk zit. Toch is het merendeel van de opgevraagde data volslagen overbodig om *Minion Rush* te spelen.

En het gaat nog verder. Tijdens het spelen van *Minion Rush* krijgen we muntjes aangeboden waarmee we verder kunnen komen in het spel. Normaal gesproken verdien je die door hard te werken of ze te kopen, maar als we ons Facebook- of Google Plus-account aan de app koppelen, krijgen we vijftig muntjes. Als we op dit aanlokkelijke bod ingaan, geven we niet alleen een lijst met wie onze Facebook- of Google Plus-vrienden zijn zomaar vrij, maar ook de aan die accounts gekoppelde contactgegevens. Op die manier hebben vermoedelijk miljoenen kinderen hun eigen of de contacten van hun ouders naar een server in de Verenigde Staten gestuurd, zonder dat zij of hun ouders dat wisten. Laat staan de vrienden van die ouders.

We testen nog meerdere kinderspelletjesapps. Steeds zijn de resultaten anders, maar is de conclusie dezelfde: zonder dat we het zien, vliegen onze data de hele wereld over en komen bij honderden verschillende bedrijven terecht.

En, weten we nu: de smartphone die voor ons op tafel ligt, is niet wat hij lijkt. Als je naar deze black box kijkt zie je een mooi ding met handige apps, maar als je onder de motorkap kijkt, zie je een systeem dat gegevens over zijn gebruiker verzamelt, rondstuurt en verkoopt aan de hoogste bieder. De smartphone blijkt een glimmend surveillanceapparaat waar je toevallig óók mee kunt bellen en appen.

Waarom dit zo ongemakkelijk voelt

Naar aanleiding van ons onderzoek naar laptops en smartphones publiceren we een serie artikelen. Veel lezers zijn – net als wij – verbluft. We vinden het *eng* dat tientallen onbekenden ons begluren. We vinden het *griezelig* dat onze gegevens in een flits worden

geveild. We zijn *verontwaardigd* dat dit alles buiten ons zicht om gebeurt. Maar waarom eigenlijk? Hoezo shockeert dit ons? Waarom zijn we boos?

In de hoop op deze vragen een antwoord te vinden, spreken we in een Brussels restaurant met filosofe Helen Nissenbaum. Deze hoogleraar aan New York University is een belangrijke stem in het hedendaagse privacydebat. Haar theorie over de contextafhankelijkheid van privacy – een van de invloedrijkste ideeën over privacy van de afgelopen tien jaar – zal in onze zoektocht een belangrijke rol spelen. En geeft antwoord op twee wezenlijke vragen: wat is privacy? En: waarom voelen wij ons soms wel en soms niet in onze privacy geschonden? Eerst maar eens een voorbeeld dat haar ideeen illustreert.

De luchthaven. Op het eerste oog is een luchthaven de privacyhel op aarde; er zijn weinig plekken waar je in korte tijd zoveel intieme informatie moet delen. Je moet jezelf aan verschillende personen identificeren; beveiligers lichten je tassen door; op sommige vliegvelden worden je vingertoppen, gezicht of irissen gescand en je kunt te allen tijde gefouilleerd worden door een onbekende beveiligingsbeambte.

Toch vliegen we er niet minder om. Sterker nog, onderzoek laat zien dat meer dan 90 procent van de 9.600 ondervraagden uit negen verschillende landen vindt dat hun privacy wordt gerespecteerd op luchthavens.[17] Komt dit doordat die meerderheid privacy niet belangrijk vindt? Nee, zegt Nissenbaum. Het komt doordat wij op de luchthaven andere privacyverwachtingen hebben dan bij de bakker. We vinden het prima als een douanebeambte onze tas inspecteert, terwijl we de bakker daarvoor een klap zouden verkopen.

Van het vliegveld tot de bakker: binnen iedere context gelden diepgewortelde privacynormen, zegt Helen Nissenbaum. Normen over de 'gepastheid van de informatiestromen' binnen die context. Deze

normen scheppen de *verwachtingen* die wij hebben over die stromen. En wanneer een van die normen wordt overtreden – wanneer de bakker wél je tas doorzoekt – ervaren wij dit als een privacyschending. Nissenbaum noemt het een veronachtzaming van de *integriteit van de context*.

Een 'recht op privacy,' zegt Nissenbaum, is dus een 'recht op gepaste stromen van persoonlijke informatie.' En ze voegt eraan toe: 'Wij ervaren alleen een privacyschending als we de informatiestroom niet gepast vinden.'

Nog een voorbeeld van Nissenbaum: een bezoek aan de huisarts. Als patiënt verwacht je dat de arts je persoonlijke informatie vertrouwelijk behandelt, maar óók dat hij die deelt met specialisten wanneer dat nodig is. Dat zijn de normen die bij deze context horen. Mocht je erachter komen dat jouw arts je gegevens aan een marketingbedrijf heeft verkocht, dan zal je die informatiestroom ongepast vinden en zijn gedrag als een grove privacyschending ervaren; de norm is overtreden, de integriteit van de context 'huisartsbezoek' geschonden.

Nissenbaum analyseert dat dan als volgt. Binnen iedere context stroomt er informatie van een zender (in voorgaand voorbeeld: de patiënt) naar een ontvanger (de arts). Deze informatiestroom heeft bepaalde kenmerken: hij heeft een onderwerp (lichamelijke klachten van de zender), is van een bepaald type (mondeling) en de voorwaarden zijn duidelijk (vertrouwelijkheid is de norm, delen met specialisten mag). Als een van deze kenmerken verandert – de ontvanger van de informatie, het soort informatie, de voorwaarden – dan is de informatiestroom niet meer gepast; dan wordt er niet voldaan aan de verwachtingen die wij hebben en wordt onze privacy geschonden.

Deze theorie verklaart waarom wij en onze lezers zo geschokt zijn door onze onderzoeksresultaten. We verwachten niet dat er 54 adverteerders over de schouders van onze kinderen meekijken als ze een spelletje spelen. We verwachten ook niet dat er veertig bedrijven over onze schouder meekijken als we het nieuws lezen.

Plotseling worden we geconfronteerd met totaal onverwachte informatiestromen naar ontvangers die wij niet kennen. Nissenbaums theorie verklaart ook waarom we onze smartphone niet *ervaren* als een allesverzengende privacyschending: we *zien* de datastromen niet. Om een stroom als ongepast te kunnen beoordelen, moet je toch tenminste zien dat hij er is.

Nissenbaums theorie biedt ons een kader om over privacy en privacyschendingen na te denken. Aan de ene kant geeft haar theorie ruimte aan nuance, door niet iedere vorm van dataverzameling per definitie af te keuren. Aan de andere kant stelt ze ons in staat om resoluut te oordelen als er overduidelijk bestaande normen worden overtreden.

In haar redenatie neemt Nissenbaum nadrukkelijk bestaande contexten als uitgangspunt. Daarmee biedt zij een krachtig tegengeluid aan het populaire argument dat online technologieën nieuwe privacynormen creëren. Zoals Facebookoprichter Mark Zuckerberg, die in 2010 zei dat mensen gewend zijn geraakt aan het openlijk delen van meer informatie en dat daardoor de 'sociale norm' van privacy is geëvolueerd. Nee, stelt Nissenbaum: bijna alles wat wij online doen, is gerelateerd aan bekende contexten. De privacynormen zijn hetzelfde als in de offline wereld.

Dus als je geld overmaakt, zegt Nissenbaum, maakt het niet uit of je die transactie per telefoon, online of bij de bank zelf doet: je mag als individu dezelfde normen hanteren over de gepastheid van de informatiestroom van jou naar de bank. Want waarom is het wel vanzelfsprekend dat de bankbediende respectvol met jouw persoonlijke informatie omgaat, terwijl de website van de bank verschillende trackers toelaat die informatie over jou verzamelen en verkopen aan commerciële partijen? De context is niet: online bankieren, met allemaal nieuwe regels. De context is: financiële transactie met de bank.

De activiteiten die we online ondernemen, lijken bijna altijd exact op wat wij in de offline wereld doen – wij doen aankopen, we maken contact met vrienden, we lezen het nieuws, we luisteren naar muziek. Maar wat er online, buiten ons zicht om, met onze persoonlijke informatie gebeurt, is – letterlijk – ongekend. Het type informatie dat over ons verzameld wordt, de vele vaak onbekende ontvangers, de manier én schaal waarop deze verzameld wordt en de redenen waarom: het is met niets uit de echte wereld vergelijkbaar.

Maar als je wilt beoordelen wat de gevolgen van dergelijke nieuwe informatiestromen zijn voor onze privacy, moet je het volgens Nissenbaum dus wel met de normen die in de echte wereld gelden vergelijken. Van vriendschap tot shoppen tot het lezen van de krant: de diepgewortelde normen die wij als samenleving hebben ontwikkeld over verschillende contexten, zouden ook maatgevend moeten zijn voor hoe wij onze privacy online beoordelen – op Facebook, bol.com of nu.nl.

In een wetenschappelijk artikel illustreert Nissenbaum dit punt door het zoeken van informatie in een bibliotheek met googelen te vergelijken: 'Ook al verschilt het zoeken op Google met het raadplegen van een bibliotheekcatalogus, er is ook een overeenkomst: beide doe je voor onderzoek, het opdoen van kennis en intellectuele verrijking. Juist deze activiteiten zijn in liberale democratieën belangrijk en moeten niet gehinderd worden door meekijkers of opdringerige autoriteiten.'[18]

Met Nissenbaums theorie kunnen we niet anders dan concluderen dat onze privacy online continu geschonden wordt. We worden continu bespied, in situaties waarin dat, als we uitgaan van vergelijkbare situaties in de fysieke wereld, volstrekt ongepast zou zijn. De meest onverwachte informatiestromen gaan van ons naar bekende bedrijven én obscure partijen. En we hebben geen idee wat zij met onze data doen.

De privacyparadox

Na het gesprek met Helen Nissenbaum weten we waar dat *unheimische* gevoel vandaan komt bij het delen van onze data. Tegelijkertijd dringt één vraag zich steeds prominenter op: kunnen wij ons tegen dat gegluur wapenen? Hoe meer we leren over de praktijken van trackers en andere digitale spionnen, hoe meer we er iets aan willen doen.

En dat doen we allebei ook wel. Nou ja, een beetje. We gaan versleuteld mailen, zodat de inhoud van onze mails niet kan worden meegelezen. Maar dat geeft een hoop gedoe, zeker als een van ons zijn encryptiesleutel verliest en berichten onleesbaar worden. We gebruiken *ad blockers*, zodat we niet meer besprongen worden door trackers als wij online gaan. Maar dan kunnen we veel sites niet meer optimaal bekijken. Ook sporen we vrienden aan de veilige berichtenapp Signal te gebruiken, maar de meesten blijven stug WhatsApp gebruiken. Facebook afzweren? Dat vinden we jammer. En laten we eerlijk zijn: meesterspion Google maakt ongeëvenaard handige en mooie dingen. Verschillende versies van dit boek zijn bijvoorbeeld in Google Docs geschreven, omdat we daarin zo fijn samen kunnen werken.

Zeker, dat kun je hypocriet noemen, of een gebrek aan ruggengraat.

Privacyexperts noemen dit de 'privacyparadox': de neiging om privacy belangrijk te vinden, maar er niet of nauwelijks naar te handelen. Een mooi voorbeeld is Facebook. Of beter: de privacyvoorwaarden van het socialemediabedrijf. Iedere keer als het bedrijf die voorwaarden aanpast – en dat doet het nogal vaak – breekt er grote onrust uit. Mensen zeggen (vaak op Facebook) dat zij nu écht gaan stoppen met Facebook omdat het bedrijf nu écht te ver gaat in zijn verzameldrift. Er worden mails rondgestuurd waarmee gebruikers hun onvrede kenbaar kunnen maken. Er verschijnen stukken in kranten en verongelijkte items op televisie. En dan?

Dan waait de storm over en blijft nagenoeg iedereen het sociale medium gebruiken.

Waarom zetten wij onze woorden niet om in daden? We schreven het al in onze inleiding: als er iets tegenover staat, zijn wij simpelweg bereid een deel van onze privacy op te geven. In de woorden van de hoofdeconoom van Google: 'Iedereen verwacht dat hij getrackt en gemonitord wordt, aangezien de voordelen van gebruiksgemak, veiligheid en geleverde diensten zo groot zijn.'[19] En zo is het.

Er zijn veel redenen om je niet te gedragen naar je privacybezorgdheid en zo de privacyparadox in stand te houden. Omdat diensten gratis zijn als je er je data aan afstaat. Omdat ze makkelijker en efficiënter in gebruik zijn. Omdat je vrienden en collega's ze ook gebruiken. Maar ook: omdat je erin berust dat je als individu nauwelijks invloed kunt uitoefenen op de praktijken van de dataverzamelaars en geen enkele controle hebt over jouw datastromen. Herkenbaar, niet?

Deze berusting is in 2015 aangetoond door professor Joseph Turow van de Annenberg School for Communication, een vooraanstaand expert op het gebied van online gedragsbeïnvloeding en auteur van het boek *The Daily You*. In een onderzoek onder 1.500 Amerikanen lieten hij en zijn onderzoeksteam overtuigend zien dat berusting – door hen gedefinieerd als 'het accepteren van iets onwenselijks dat tegelijkertijd onvermijdelijk is' – een belangrijkere verklaring is voor de privacyparadox dan het feit dat wij bereid zijn om privacy in te ruilen voor iets anders.[20] 84 procent van de ondervraagden verklaarde privacy belangrijk te vinden, bijna 60 procent berustte erin niets aan het verlies van privacy te kunnen doen. De saillantste vondst: 41 procent van de ondervraagden berustte niet alleen in die machteloosheid, maar was ook nog eens van mening dat zij persoonlijke *schade* door al die verzamelende partijen zouden ondervinden.

De ongeïnformeerde gebruiker

Een andere belangrijke verklaring voor de privacyparadox is een gebrek aan informatie. Zelfs als je als gebruiker het naadje van de kous wilt weten, is het vaak onmogelijk om erachter te komen wat er exact met de data gebeurt die deze bedrijven over jou verzamelen.

Tijdens ons onderzoek naar de trackers ontdekken wij dat veel databedrijven simpelweg niet bekendmaken wat zij met onze data doen. We lezen de privacyvoorwaarden door en kijken op hun websites, maar daar is lang niet alles te vinden.

Dus doen we navraag bij de beheerders van sites als nu.nl, telegraaf.nl en voetbalzone.nl. Zij zijn degenen die het overzicht hebben over wat er op hun sites gebeurt. Maar tot onze grote verbazing weten ook zij niet precies door welke trackers hun bezoekers worden gevolgd. 'Ik heb geen enkel zicht op wat derde partijen op onze site allemaal voor informatie meetrekken. Ik vertrouw erop dat die bedrijven zelf hun verantwoordelijkheid nemen,' antwoordt een webmaster van een Nederlandse site met honderdduizenden bezoekers per maand, die anoniem wil blijven. Sanoma, de uitgever van nu.nl, laat weten dat het bedrijf niet 'de rol van de toezichthouder' op zich kan nemen bij het controleren van trackers. Ja, zegt het hoofd Digital Advertising, Sanoma kiest 'zorgvuldig' zijn partners uit, maar het is onmogelijk om exact na te gaan wat de trackers doen. 'Als je alles zou checken, kun je de zaak wel opheffen.'

Als zelfs verantwoordelijken voor websites en apps geen idee hebben door wie hun bezoekers worden bespioneerd, hoe kun je als gebruiker dan ooit op de hoogte zijn van wat al die trackers doen en waar al je data heen gaan?

Opvallend genoeg staat de zogenoemde 'geïnformeerde gebruiker' in de privacywetgeving juist centraal. Als gebruikers informatie hebben over hun datastromen, zo is de gedachte, kunnen zij zelf een beslissing nemen of zij daar wel of niet mee akkoord gaan. Zo eist de Nederlandse wet dat bedrijven klanten en bezoekers

informeren over de verwerking van persoonlijke gegevens – middels de algemene én privacyvoorwaarden. En zijn websites sinds de aanpassing van de Nederlandse Telecommunicatiewet (cookiewet) verplicht hun bezoekers vooraf te informeren welke gegevens er op hun site worden verzameld en moeten zij toestemming vragen voordat ze een cookie plaatsen.

Een geweldig idee. Maar in de praktijk een totale wassen neus. Ga maar na: nu.nl plaatst 44 verschillende cookies. De informatie die daarmee wordt verzameld, wordt doorgestuurd en verkocht aan nog eens tientallen andere bedrijven. Welke bedrijven geïnteresseerd zijn in die datastromen, wat ze ermee doen en op grond waarvan, is zo'n ingewikkeld technisch én juridisch verhaal dat het nauwelijks uit te leggen valt – mocht nu.nl zelf weten wie die bedrijven zijn en wat ze doen, wat ze dus niet weten.

Zeker, in de befaamde *terms and conditions* en privacyvoorwaarden doen bedrijven een poging om hun gebruikers voor te lichten over hoe hun data worden gebruikt. Maar uit veel onderzoek blijkt dat wij die dingen niet lezen. Onderzoekers van de Carnegie Mellon-universiteit berekenden al in 2008 dat wanneer de gemiddelde Amerikaan alle privacyvoorwaarden zou lezen, hij daar jaarlijks vijf volle werkweken mee bezig zou zijn. Ter illustratie: de terms and conditions van PayPal zijn langer dan Shakespeares *Hamlet*. Die van iTunes tellen meer woorden dan *Macbeth*. Dezelfde onderzoekers berekenden dat als iedere Amerikaan de voorwaarden op de sites die hij bezoekt helemaal zou lezen, dit de Amerikaanse economie in totaal 781 miljard dollar per jaar zou kosten.

Deze cijfers onderstrepen wat iedereen al weet. *Niemand leest de privacyvoorwaarden.*

Het kost bizar veel tijd en we begrijpen ze toch niet. We zijn gekke Henkie niet. Daarom gaan we allemaal slaafs akkoord met de voorwaarden, zoals Nederlanders ook allemaal de cookietoestemmingsverzoeken klakkeloos accepteren.

Gesteld dat de privacyvoorwaarden wél duidelijk zijn, wij ze zouden lezen én begrijpen, dan nog is er vaak geen echte keuze. Als je het bijvoorbeeld niet eens bent met de toestemmingen die de Bijenkorfapp vraagt en de voorwaarden weigert, kun je de app niet gebruiken. Datzelfde geldt voor de zogenoemde '*cookie walls*' op sites: je móét wel op 'ik ga akkoord' klikken, anders werkt de site niet goed. Vaak staan de privacyvoorwaarden in de algemene voorwaarden. Als je daar niet mee akkoord gaat, krijg je geen toegang.

Zo blijven we – omdat het makkelijk is, omdat het gratis is, omdat het efficiënter is, omdat we erin berusten, omdat we het niet weten, omdat we het niet begrijpen of omdat we simpelweg geen keuze hebben – onze privacy belangrijk vinden zonder aan de schending ervan echt wat te kunnen doen.

Het onderscheid tussen de privé- en publieke ruimte vervaagt

Maar er is meer aan de hand. Dat leren wij als wij Bert-Jaap Koops in zijn woning in Amsterdam interviewen. Deze hoogleraar Regulering van Technologie aan de Universiteit van Tilburg is een van de scherpste Nederlandse denkers over privacy die wij kennen. Zijn denken is eclectisch en zijn blikveld is breed – zo bestudeerde hij de afgelopen jaren DNA-databanken, versleuteling van communicatie, digitale grondrechten en genetica. Zijn verhaal? Volgens Koops hebben technologieën als de smartphone ertoe geleid dat het privacyrecht hopeloos verouderd is.

Van oudsher, zegt hij, speelt het onderscheid tussen 'private' en 'publieke' ruimte een essentiële rol in het privacyrecht. Kort gezegd: dat wat wij als de private ruimte beschouwen, is door wet- en regelgeving goed beschermd. In de publieke ruimte speelt privacyrecht daarentegen nauwelijks een rol: daar geldt volgens de wetboeken 'geen redelijke verwachting van privacy.'

Met andere woorden: in je huis ben je op privacygebied goed beschermd door wet- en regelgeving en vanaf het moment dat je de deur achter je dichttrekt niet meer.

Maar dit onderscheid, zegt Koops, kan in de huidige tijd niet anders dan 'wereldvreemd' worden genoemd. De hoogleraar geeft daar twee argumenten voor.

'Allereerst neem je tegenwoordig een groot deel van je huis mee als je naar buiten gaat,' legt hij uit. 'In je smartphone staan je mailcorrespondentie, je fotoalbums, je adressenboekje. Je huis is niet meer bij uitstek de plek waar je privédingen doet, zoals dat vroeger wel het geval was.' Tegelijkertijd zijn er nu allemaal partijen die binnenshuis ons gedrag registreren. Denk aan de trackers op onze laptop en smartphone. Of de smartmeter die ons energiegebruik registreert en naar de producent stuurt. 'Het huis erodeert als de plaats van privacy,' zegt Koops.

Ten tweede, legt hij uit, staat een andere kern van het privacyrecht op losse schroeven: het idee dat wij ons relatief anoniem door de publieke ruimte kunnen bewegen. Zodra wij buiten zijn, worden wij door allerlei apparaten geregistreerd en worden onze gangen gevolgd. Denk aan de wifitrackingtechnologieën die winkels inzetten om klanten te herkennen en steden als Utrecht, Eindhoven en Amsterdam inzetten om mensenstromen te analyseren. Of denk aan het feit dat onze smartphone continu onze locatie doorgeeft aan tientallen zendmasten. En wat te denken van al die camera's die in de publieke ruimte hangen? De gezichtsherkenningssoftware wordt met de dag beter. Gezichten die in de publieke ruimte worden gefotografeerd zullen binnenkort herkend kunnen worden. Weg anonimiteit. 'De facto,' zegt Koops, 'ben je dan in het openbaar altijd te identificeren.'

Dit is nogal wat. Ons hele denken over privacy is gebaseerd op het onderscheid tussen privé- en publieke ruimte. Een onderscheid dat betekenisloos aan het worden is. Koops is om die reden nu

druk met zijn hoogst ambitieuze academische project: het uitdenken van wat hij het 'huisrecht 2.0' noemt, een vorm van privacybescherming die het publiek-privéonderscheid loslaat. 'Volledige controle over je digitale gegevens gaat niet werken,' zegt Koops, 'maar ik vind het interessant om na te denken of je wel controle zou kunnen krijgen over een ruimte in de digitale wereld waar alleen jij de beschikkingsmacht over hebt. Een soort digitaal huis met virtuele muren om jouw digitale gegevens heen. En waar jij het zogeheten 'ius excludendi' kunt uitoefenen: die wil ik binnen hebben en die niet.'

Een bijzonder interessant idee. Maar het is precies nog dat: een idee, waar Koops nog drie jaar aan denkt te moeten werken. Ondertussen blijft de buitenwereld bij ons binnenkomen.

En die buitenwereld bestaat niet alleen uit adverteerders die hopen met onze data geld te kunnen verdienen. Ook overheden jagen op onze data en proberen die – legaal of niet – te verkrijgen. En ook cybercriminelen worden steeds vernuftiger. Lang dachten we dat waarschuwingen over krakkemikkige cybersecurity een commercieel trucje waren van beveiligingsbedrijven die een nieuwe markt wilden aanboren. Totdat we ons gingen verdiepen in de veiligheid van het internet waar we zoveel van onze data aan toevertrouwen.

NSA's geheimen van nu zijn het onderwerp van de promovendi van morgen en de hackertrucks van overmorgen.'[21]

– BEVEILIGINGSEXPERT BRUCE SCHNEIER

'In de toekomst kunnen geheime diensten het internet der dingen gebruiken voor identificatie, surveillance, monitoring, locatieopsporing, werving van bronnen en om toegang te krijgen tot netwerken en persoonsgegevens.'[22]

– DIRECTOR OF NATIONAL INTELLIGENCE VS JAMES CLAPPER

2

Hackers en de NSA

Waarom ieders persoonlijke gegevens fundamentele risico's lopen

We zien een doorsnee woonkamer. Links een tuindeur, rechts een open keuken. In het midden van de kamer een bank, een glazen bijzettafel en een kastje. In de tuin zien we een wat oudere man rommelen. Aan de keukentafel zit een vrouw van vergelijkbare leeftijd. Naast haar staat een jonge vrouw die een meisje helpt met viltstiften en papier. Vanuit ons perspectief lijkt het een kleurplaat waar ze mee bezig is. Het zou ook een brief of een tekening kunnen zijn.

We passen ons beeld aan. Tikkie naar rechts, stukje naar onderen. Inzoomen. Bingo. Kleurplaat.

We kijken verder. We zien schilderijen aan de muur en pannen in de keukenkast. We bekijken het parket op de vloer en de schaduwen op het plafond. Dan zetten we het geluid aan. Dat is blikkerig, maar de gesprekken zijn goed verstaanbaar. We horen het gezelschap lachen, praten en lopen.

Dit voelt vreselijk ongemakkelijk.

Waarom in hun woonkamer een camera hangt, weten we niet. Wie deze mensen zijn en waar ze wonen, ook niet. We weten wél welk merk camera zij bezitten, wat het typenummer is en welke software erop draait. Ook bekend: de gebruikersnaam en het wachtwoord, waarmee van afstand op de camera kan worden ingelogd. En dat is precies wat we hebben gedaan. We zien op onze laptop wat het oog van de camera registreert. We kunnen zelfs de camera besturen en de instellingen veranderen. Zodat de camera bijvoorbeeld 's nachts uitgaat.[23]

We hebben getwijfeld of we dit experiment moesten doen. We zijn inbrekers, voyeurs, hackers en journalisten tegelijk. Maar we hebben besloten de morele en juridische grenzen voor een paar uur te overschrijden. Dit is de enige manier om dit verhaal te vertellen. Het verhaal over de veiligheid van het internet. En daarmee over de veiligheid van onze persoonlijke data.

In het eerste deel van onze zoektocht probeerden we laptops en smartphones te doorgronden en onze datastromen in kaart te brengen. Wij ontdekten dat we veel gegevens kwijtraken zonder dat we het doorhebben. Dit verlies is *bedoeld*: adverteerders, softwareontwikkelaars en smartphonebouwers hebben de techniek zo ontworpen dat onze data gebruikt, verkocht en verhandeld kunnen worden. We raken onze gegevens kwijt, omdat de technologie werkt.

Nu zetten we de volgende stap: Welke gegevens raken we *onbedoeld* kwijt, door slordigheid, diefstal, sabotage, mankementen en ongelukken? Hoe omzeilen hackers en spionerende overheden de beveiliging van de computers, systemen en netwerken waar wij allemaal – bewust of onbewust – onze persoonlijke gegevens aan afstaan?

We hacken het internet der dingen

Onze eerste gids in deze technische jungle is Wouter Slotboom, beveiligingsexpert en ethisch hacker. Op Slotbooms advies maken wij gebruik van Shodan, een openbare zoekmachine, die wel 'de Google voor hackers' wordt genoemd. Waar Google de inhoud van webpagina's ontsluit, biedt Shodan informatie over apparaten die op het internet zijn aangesloten. Shodan is een portaal naar het zogenoemde *Internet of Things*, de ontwikkeling dat steeds meer fysieke objecten aan het internet worden gehangen. Printers, webcams, televisies, externe harde schijven, geluidsinstallaties, thermostaten: we willen ze *wireless*, *connected* en *remote accessible*.

Samen met Slotboom testen we de veiligheid van dit internet der dingen. Gewoon, vanachter onze computer. Eerst stellen we een aantal regels op:

- We doen ons onderzoek binnen één werkdag.
- We proberen verschillende soorten apparaten over te nemen, zoals camera's, industriële systemen en infrastructuur.
- We gaan steekproefsgewijs te werk.
- We maken geen gebruik van geavanceerd hacken; alles wat we doen moet voor iedereen herhaalbaar zijn.
- Komen we iets tegen wat een direct gevaar oplevert – bijvoorbeeld een energiecentrale die van een afstand is te besturen – dan lichten we die partij eerst in voordat we publiceren. We willen geen kwaadwillende hackers wakker maken.

We beginnen met beveiligingscamera's. We zoeken in Shodan op een aantal bekende cameramerken voor de consumentenmarkt. Deze camera's kosten vaak niet meer dan honderd euro en zijn eenvoudig te installeren. Door die camera's aan het internet te verbinden, is het mogelijk ze vanaf verschillende apparaten te bekijken. Handig voor de snackbarhouder die thuis op zijn tablet zijn zaak in de gaten wil houden. Of voor ouders die tijdens een avondje uit op hun smartphone hun kind rustig willen zien slapen.

Met tien zoekacties in Shodan vinden we wereldwijd elfduizend camera's waarop we kunnen meekijken. We zien al direct dat veel van de camera's namen hebben gekregen. 'Opa en Oma cam,' bijvoorbeeld. Of: 'Voordeur.' Sommige camera's zijn goed met een wachtwoord beveiligd, andere hebben helemaal geen wachtwoord. We krijgen dan van Shodan een IP-adres, plakken dat in onze browser en kunnen meekijken. Weer andere camera's hebben nog steeds het wachtwoord dat de fabrikant standaard meegeeft. Heel vaak is dat: admin/admin. Of: admin/1234. Sterker: je kunt op

Shodan zoeken naar alle apparaten die zélf aangeven dat ze dergelijke fabrieksinstellingen hebben. Dat zijn er schrikbarend veel. 'Dit is vergelijkbaar met je huissleutel onder de mat leggen en een briefje op de voordeur hangen met de tekst: 'De sleutel ligt onder de mat',' zegt Slotboom ter vergelijking.

Onder zijn begeleiding doen we een steekproef bij 25 camera's uit de resultatenlijst. Bij tien daarvan krijgen we beeld. Na de hiervoor beschreven woonkamer bekijken we een babykamer, een kapperszaak en een gokhal. We zien de voor- en achterdeur van een huis, een onbestemde kantoorruimte, een pandjeszaak en een ijssalon waar een meisje net een ijsje koopt.

Wat belangrijk is om te vermelden: wij doen deze hacks handmatig en willekeurig. Een programmeur kan heel eenvoudig geautomatiseerd zoeken naar onbeveiligde camera's en in luttele seconden bij iedereen inloggen en naar binnen kijken. Als die slim zoekt, kan die bijvoorbeeld snel de interessante plaatsen uit de resultatenlijst halen: banken, overheidsgebouwen, slaapkamers. Nogal handig voor inbrekers of andere kwaadwillenden.

Daarna zoeken we met Slotboom naar printers. Hartstikke handig om draadloos te kunnen printen, maar zonder beveiliging kunnen er gevaarlijke situaties ontstaan. Wij zoeken weer naar de bekende merken en vinden bijna elfduizend apparaten. We doen een steekproef. Sommige printers zijn beveiligd, maar bij andere zitten we direct in het apparaat. We zouden de instellingen kunnen aanpassen, zien welke printopdrachten op dit moment worden uitgevoerd en die stopzetten. In sommige printers zit een opslagfunctie, waardoor we de printgeschiedenis kunnen inzien. En we zouden ook zelf opdrachten kunnen geven en documenten uit de printer laten komen. Ernstiger is dat de printer voor geoefende hackers een ingang is. Via de printer kunnen ze verder het netwerk van de eigenaar verkennen en in andere apparaten komen. Gevaarlijke situaties.

We nemen contact op met Hewlett-Packard, het merk waarvan we 1.325 apparaten vinden die zonder wachtwoord door ons te

hacken zijn. Een woordvoerder benadrukt dat de veiligheid van de klanten heel belangrijk is voor Hewlett-Packard. 'Daarom sporen we klanten aan om printers veilig te gebruiken.' Dat 'aansporen' doet Hewlett-Packard door gebruikers op hun site te informeren. En: 'Bij de nieuwe printerseries hebben we deze informatie ook toegevoegd aan de installatiehandleiding.'

Omdat we zo lekker bezig zijn, gaan we door naar het volgende apparaat: de externe harde schijf. Juist, dat ding waarop je belangrijke documenten, foto's en andere zaken zet die niet verloren mogen gaan. Of die je uit privacyoverwegingen niet online wilt opslaan maar die je wel lekker gemakkelijk thuis via je eigen netwerk wilt bekijken. We vinden duizenden back-upservers die aan het internet zijn gekoppeld, vaak zogenoemde *network-attached storage* (NAS)-schijven. En ook hier blijkt uit onze kleine steekproef dat we bij ongeveer één derde van de schijven gewoon binnenkomen. We hebben toegang tot vakantiefoto's, notariële akten en contracten van bedrijfsovernames. We zien paspoorten en diploma's, jaarrekeningen en patenten.

Eind 2012 maakte het televisieprogramma *KRO Reporter* een reportage over online printers, back-upservers en camera's.[24] Een van de apparaten die het programma onder de loep nam, was de populaire NAS-schijf van Iomega, een onderdeel van technologiebedrijf Lenovo. Daarop werden onder andere patiëntgegevens van artsen en correspondentie van de Koninklijke Marechaussee gevonden. Na die uitzending beloofde Iomega een software-update om het probleem te verhelpen.

Via Shodan vinden wij in Nederland nog steeds 1.119 Iomega-schijven zonder login en wachtwoord. Een woordvoerder van Lenovo vertelt ons dat Iomega sinds de uitzending is gaan werken met een ingebouwd standaardwachtwoord in de NAS-schijven. Toch vinden wij wereldwijd nog 15.202 exemplaren zonder wachtwoord. Bovendien is het standaardwachtwoord via Google simpel te achterhalen. De woordvoerder benadrukt dat de verantwoordelijkheid voor beveiliging uiteindelijk bij de gebruiker zelf ligt.

Dat brengt ons bij het laatste huis-tuin-en-keukenapparaat dat wij met Slotboom onderzoeken: de router. Routers zijn gekoppeld aan een modem, die verbinding maakt met het internet. Via Shodan zijn er honderdduizenden routers te vinden. We ontvangen informatie over het merk, het typenummer en de wijze van beveiligen.

Hierdoor hebben we toegang tot mogelijk duizenden routers. En als je eenmaal toegang hebt, kun je bijvoorbeeld al het internetverkeer van die gebruiker omleiden en opvangen. Dit is een beproefde truc van criminelen. Zij dringen routers binnen en sturen gebruikers die willen internetbankieren naar neppe banksites. Met alle gevolgen van dien.

Andere boeven voegen iemands router toe aan een zogenoemd botnet. Dat is een 'leger' van geïnfecteerde computers die onder controle van een crimineel staan en gebruikt worden om spam te versturen, malware te verspreiden of aanvallen uit te voeren op webservers. Zo wordt dat apparaat in je bezemkast een wapen in handen van een kwaadwillende hacker.

Het beeld na een dagje Shodan met Slotboom is glashelder. Veel apparaten die wij aan het internet hangen zijn lek, waardoor onze data potentieel tot prooi zijn verworden. Soms ligt dat aan de fabrikant en soms ligt het aan onszelf. Maar net als bij de smartphone en de laptop geldt ook hier dat we dit niet zien. Er is een hackingtool als Shodan nodig om de onveiligheid die zich onder de oppervlakte bevindt, bloot te leggen. We zien slechts een beveiligingscamera die onze woonkamer bewaakt, een externe harde schijf waarmee wij overal onze privéfoto's kunnen bekijken en een router die ons internet bezorgt. Wat wij niet zien, zijn de kiertjes in deze zwarte dozen die openstaan en ongewenste indringers toegang bieden tot ons privéleven. Niet voor niets vertelde James Clapper, het hoofd van de Amerikaanse inlichtingendiensten, in 2016 het internet der dingen als grote kans voor zijn diensten te zien.

We dringen openbare wifinetwerken binnen

We trekken ook met Slotboom naar buiten. We hebben hem gevraagd om met ons de publieke ruimte te verkennen, om te kijken wat we allemaal van mensen in die ruimte te weten kunnen komen.[45]

We spreken af op een terras in Amsterdam. Het is zonnig, bijna alle tafels zijn bezet. Sommige terrasbezoekers praten met elkaar, anderen werken op hun laptop of zitten op hun smartphone. In de rugzak van Slotboom zit een klein zwart apparaat, iets groter dan een sigarettenpakje, met een antenne eraan. Het is een WiFi Pineapple, een apparaat dat je voor ongeveer honderd euro online kunt kopen. Slotboom pakt zijn laptop uit zijn rugzak, legt de Pineapple op tafel en verbergt hem onder een menukaart. We bestellen koffie bij de serveerster en vragen het wachtwoord van het wifinetwerk. Intussen zet Slotboom zijn laptop en de Pineapple aan. Hij start wat programma's op en zijn scherm vult zich met regels groene tekst.

Langzaam wordt ons duidelijk dat de laptops, smartphones en tablets van de terrasbezoekers contact leggen met het apparaatje. Op Slotbooms scherm verschijnen woorden als 'iPhone van Joris' en 'MacBook van Simone.' De antenne van de Pineapple vangt de signalen op die de laptops, smartphones en tablets afgeven. Ook van sommige voorbijgangers.

Er verschijnt meer tekst op het scherm. We kunnen nu van alle apparaten die contact hebben gemaakt met de Pineapple achterhalen op welke wifinetwerken ze eerder ingelogd zijn geweest. Soms zijn dat onherleidbare namen met veel cijfers en letters, vaker dragen de wifinetwerken namen van de locatie waar ze bij horen. We zien dat dezelfde Joris een McDonald's heeft bezocht, waarschijnlijk in Spanje of Zuid-Amerika is geweest (veel Spaanstalige netwerknamen) en bij een bekend kartcentrum in het westen van het land heeft ingelogd. Een andere terrasbezoeker, een zekere Martin, is ingelogd geweest op het netwerk van vliegveld Heathrow en dat van de Amerikaanse vliegtuigmaatschappij

Southwest. Aan de naam van het wifinetwerk te zien, slaapt hij waarschijnlijk in het White Tulip Hostel in Amsterdam. Hij heeft ook coffeeshop The Bulldog bezocht.

Nadat de serveerster ons koffie heeft gebracht, legt Slotboom uit waarom hij dit kan zien. Hij kan het hele terras van internet voorzien én al het internetverkeer door het apparaat laten stromen. De meeste smartphones, laptops en tablets zoeken automatisch naar een wifinetwerk. Het liefste vinden ze er een waar zij al eerder op aangesloten zijn geweest. En Slotbooms Pineapple is in staat zich voor te doen als een van die vertrouwde wifinetwerken.

We zien bijvoorbeeld dat in de lijst van beschikbare netwerken op onze smartphones ineens de namen van onze thuisnetwerken verschijnen, die van ons werk en van een hele reeks openbare plekken die we hebben bezocht (cafés, hotellobby's, treinen). De telefoons loggen automatisch in op een van deze netwerken, die dus in werkelijkheid allemaal bij de Pineapple horen. Slotboom kan een netwerk ook een gefingeerde naam geven, waardoor de gebruikers denken dat ze aangesloten zijn op het netwerk van het café. Als een café bijvoorbeeld een wifinetwerk heeft met willekeurige letters en cijfers ('FRITZBOX XYZ123'), dan kan Slotboom het netwerk de naam van het café geven ('Starbucks'). Daar loggen mensen veel sneller op in, vertelt hij.

Inderdaad: steeds meer terrasbezoekers loggen in op ons netwerk. De sirenenzang van het kleine zwarte apparaat is onweerstaanbaar. Al twintig smartphones en laptops zijn ermee verbonden.

Dat openbare wifinetwerken onveilig zijn, is geen nieuw verhaal. Het is wel een verhaal dat niet vaak genoeg verteld kan worden. Er zijn in Nederland ongeveer twaalf miljoen smartphones. Naar schatting hebben bijna tien miljoen Nederlanders een laptop. Grote kans dat nagenoeg iedere Nederlander met een van die draagbare apparaten weleens ingelogd is geweest op een openbaar wifinetwerk. In het café, de trein of in een hotel.

Er zijn maatregelen te treffen om je internetverkeer beter te beschermen als je een wifinetwerk opgaat. Bovendien zijn sommige wifinetwerken beter beveiligd dan andere. Loop een dag met Slotboom door de stad en je komt erachter dat zo ongeveer iedere smartphone, tablet en laptop via een omgeleid wifinetwerk te kraken valt. Het Nationaal Cyber Security Centrum (NSCS) adviseert niet voor niets: 'Het is af te raden in openbare plaatsen van een publiek wifinetwerk gebruik te maken.'

Bewapend met Slotbooms Pineapple verplaatsen we ons naar een koffiezaak die niet alleen bekendstaat om de prachtige bloemetjes op het melkschuim van de caffè latte, maar ook om de vele zzp'ers die er overdag op hun laptop zitten te werken. De vestiging is afgeladen met mensen die geconcentreerd naar hun beeldscherm turen. Slotboom start zijn Pineapple en laptop weer op. Er gebeurt exact hetzelfde als op het terras: binnen een paar minuten zijn er een stuk of twintig apparaten verbonden met zijn Pineapple.

Deze keer gaan wij een stap verder. Slotboom start Wireshark op, een programma dat datapakketjes onderschept en openbreekt. Hij is nu in staat om veel meer informatie over de aanwezige smartphones en laptops te achterhalen. Zo zien we nu de telefoontypen (bijvoorbeeld: iPhone 4s), de taalinstellingen van de verschillende apparaten, of de versie van het besturingssysteem (bijvoorbeeld iOS 7.0.5). Dat laatste is enorm waardevolle informatie voor een kwaadwillende hacker: als een apparaat een verouderd besturingssysteem heeft, zijn er online altijd zwakheden in het beveiligingssysteem te vinden. Via die zwakke plekken kun je het apparaat binnendringen en overnemen. Een steekproef in de koffiezaak wijst uit dat geen van de aanwezige apparaten de recentste beveiligingsupdates heeft gedownload en dat in al deze systemen zwakheden te vinden zijn.

Op Slotbooms laptop kunnen we via Wireshark nu ook het internetverkeer van de aanwezigen zien. We zien dat iemand met een MacBook nu.nl bekijkt. Op Slotbooms scherm verschijnt de

naam van een apparaat dat bezig is om via WeTransfer documenten te versturen of contact te maken met Dropbox. We zien dat iemand net is ingelogd op Foursquare. De naam van deze persoon verschijnt ook in beeld. We googelen hem en zien dat hij een paar meter van ons vandaan zit.

Zelfs van de aanwezigen die niet aan het werk of aan het surfen zijn, komt informatie binnen. Veel mailprogramma's en apps maken constant contact met hun server. Dat is nodig om, bijvoorbeeld, nieuwe e-mails op te halen. Van sommige apparaten kunnen we zelfs zien welke informatie er naar welke server wordt gestuurd. En nu wordt het echt intiem: we zien dat een van de aanwezigen de app van homodatingsite Grindr op zijn smartphone heeft staan. We zien de naam van zijn smartphone en het type (iPhone 5s). We doen het niet, maar met een beetje creatief googelen zouden we eenvoudig kunnen achterhalen om welke koffiedrinker het gaat.

Ook zien we op de laptop de voor- en achternaam van een vrouw verschijnen. Ze maakt gebruik van de site Delicious, een sociaal netwerk waar gebruikers interessante links met elkaar kunnen delen. De pagina's van Deliciousgebruikers zijn openbaar, toch voelen we ons voyeurs als we zien hoeveel we aan de hand van deze informatie over de vrouw te weten kunnen komen. We googelen haar naam, waardoor we direct op basis van haar foto kunnen bepalen wie het is en waar ze in de koffiezaak zit. We komen erachter dat ze uit Polen komt en pas sinds kort in Nederland woont. We zien dat ze geïnteresseerd is in yoga, een aanbieding voor een antisnurkmatras heeft opgeslagen, recent in Thailand en Laos is geweest en opvallende interesse toont voor sites die tips geven hoe je een relatie kunt redden. En het is maar goed dat we met elkaar fluisteren: we ontdekken dat ze een paar maanden geleden een site van een taalcursus Nederlands heeft opgeslagen én een site met informatie over de Nederlandse inburgeringscursus.

Slotboom laat ook nog wat hackertrucjes zien. Zo kan hij via een app op zijn telefoon de opdracht geven dat iedereen die een bepaald woord op een site tegenkomt (bijvoorbeeld 'Van der Steur') een ander woord te lezen krijgt (bijvoorbeeld 'Dutroux'). Of dat iedereen die een foto op een bepaalde site laadt een beeld te zien krijgt dat door Slotboom is uitgekozen.

Grappig als je kattenkwaad wilt uithalen. Het kan ook griezelig worden, zo lieten twee Berlijnse kunstenaars in 2011 zien. Danja Vasiliev en Julian Oliver, de drijvende krachten achter het hackerscollectief Critical Engineers, lanceerden toen hun project *Newstweek*.[46] In verschillende Europese koffiebars verstopten ze apparatuur vergelijkbaar met onze Pineapple die alle dataverkeer naar een centrale computer in Berlijn stuurde. Ze konden daardoor direct meekijken met wat gasten van die koffiebars op internet aan het bekijken waren. Ze konden ook nieuwsberichten, titels en foto's aanpassen die koffiedrinkers aan het bekijken waren.

Veel kwaadwillende hackers doen eigenlijk hetzelfde. Ze vangen het internetverkeer van een slachtoffer af. Als die wil internetbankieren, sturen de criminelen dat slachtoffer ongemerkt door naar een nepsite, vanwaar ze de inlogcodes kunnen stelen.

Even later, in een ander café, zal Slotboom dat ook bij ons doen. We surfen naar sns.nl, digid.nl, Facebook en live.com en komen, zonder dat we er erg in hebben, uit op een site van hem. De gegevens die we daar achterlaten, komen op een server van Slotboom terecht. Binnen twintig minuten slaagt hij erin onze inloggegevens en wachtwoorden te bemachtigen.

De boodschap is nu wel overgekomen.

We zoeken de criminele kant van het internet op

Spectaculaire hacks waarbij grote hoeveelheden persoonlijke data worden ontvreemd, zijn aan de orde van de dag. Van vreemdgangerswebsite Ashley Madison werden miljoenen gegevens van overspeligen gestolen en openbaar gemaakt. Er zouden, volgens de Canadese politie, zelfs mensen uit schaamte zelfmoord hebben

gepleegd na deze onthulling. Grote winkelketens en zorgverzekeraars verloren door hacks bij elkaar honderden miljoenen creditcardgegevens en dossiers van klanten. Het Amerikaanse Office of Personnel Management (OPM), dat de personeelsdossiers van tientallen miljoenen (oud-)ambtenaren beheert, raakte deze zeer gevoelige data kwijt in een spectaculaire hack. En eind 2015 werd datamakelaar Experian gehackt, die gegevens over miljoenen consumenten wereldwijd verzamelt, opkoopt en doorverkoopt. Hierbij zijn de persoonlijke gegevens van vijftien miljoen mensen buitgemaakt.

Voor ons onderzoek is dit een belangrijke vraag: wat gebeurt er met al die buitgemaakte data? Waar gaan ze naartoe? Om dat uit te vinden, besluiten we af te dalen in de ondergrondse wereld van de online criminaliteit.

We shoppen op het dark web

De laatste jaren is er een ondergronds internet ontstaan: het *dark web*. Dit deel van het internet is alleen te betreden met Tor, een browser die je internetverkeer anonimiseert. Hierdoor is van sites én gebruikers op het dark web niet te achterhalen waar ze zich bevinden. Daardoor kun je er anoniem blijven en op allerlei bijzondere markten illegale producten kopen en verkopen: van drugs tot gestolen persoonlijke data, van creditcardinformatie tot medische gegevens.[27]

We downloaden de Tor-browser en surfen naar de volgende letter-en-cijferbrij: http://trdealmgn4uvm42g.onion. We bevinden ons nu op TheRealDeal, een *dark market* die gespecialiseerd is in gestolen data en malware. Onder het kopje 'creditcards' zien we honderden aanbiedingen. We kunnen bijvoorbeeld gestolen kaartinformatie in bulk kopen en specifiek het land kiezen waar de creditcardinformatie is gestolen. Achter iedere aanbieding staat een rode bestelknop.

De eerste verkoper, Professor Dark, krijgt goede recensies van andere gebruikers. We besluiten bij hem informatie over een gestolen Nederlandse creditcard te kopen. Geen probleem. Dertien euro, te betalen in Bitcoin. Alsof we een Roti Kip Speciaal bestellen via Thuisbezorgd.nl, zo simpel.

We duiken in de gekochte creditcardinformatie. Die leidt naar een zekere Ronald Hoogland. Als we hem op zijn werk bellen (zijn werkmail staat in de gekochte informatie), bevestigt hij dat zijn creditcard is gestolen. Een paar maanden eerder is zijn rekening geplunderd. Er is geld uitgegeven op een goksite en aan telefoons. Hoogland heeft zijn kaart direct geblokkeerd en zijn wachtwoorden gewijzigd. Wij kunnen dus niet zoveel meer met deze gekochte informatie. We zijn opgelicht door Professor Dark.

Op de dark markets vinden we vooral kruimeldieven en amateurs. Nu willen we zien wat de echte criminelen verkopen en aanbieden. Spionagesoftware, waarmee je toetsaanslagen van iemand kunt onderscheppen bijvoorbeeld. Of een professioneel botnet dat virussen verspreidt waarmee gegevens onderschept kunnen worden als mensen gaan internetbankieren.

We spreken af met de Australiër Mark Arena, eigenaar van Intel 471, een cybersecuritybedrijf dat informatie verzamelt over internetcriminelen. In een restaurant aan het Leidseplein in Amsterdam vertelt hij dat hij ons niet in contact kan brengen met echte criminelen. Die zitten op besloten fora waar je niet zomaar opkomt.

Hoe komt Arena dan wel zo'n forum binnen als hij dergelijke figuren moet opsporen? Door mensen in te huren die dicht op de markt zitten, legt hij uit. Zo zit er een onderzoeker in Kiev, omdat die Oekraïens, Russisch én straattaal spreekt. Door veel op andere fora rond te hangen, leren Arena's onderzoekers mensen kennen die toegang hebben tot besloten groepen. Als er, soms na maanden pas, een vertrouwensband begint te ontstaan, kan een uitnodiging volgen.

Dat het vaak lukt om die vertrouwensband op te bouwen en dan te infiltreren, heeft met de organisatiestructuur van de fora te maken. Arena: 'Het idee van *The Sopranos*, waarbij onderknuppels het werk doen en het geld afstaan aan hun bazen, gaat niet op voor online criminaliteit. Vaak is er niemand de baas en zijn er vooral samenwerkingsverbanden die gesmeed en weer verbroken worden,' zegt Arena.

Een samenwerkingsverband dat '*pay per install*' aanbiedt bijvoorbeeld. Hoe dat werkt: een groep criminelen beheert een verzameling gekaapte computers, vanwaaruit ze andere computers op bestelling besmetten. Andere criminelen kunnen vervolgens op die computers malware installeren die bankgegevens onderschept. De kosten voor die te installeren besmettingen verschillen per regio: van zo'n honderd dollar voor duizend besmettingen in West-Europa tot zo'n zeven à acht dollar voor duizend besmettingen in Azië.

Los van de samenwerkingsverbanden zijn er nog de honderden freelancers die zich op de fora aanbieden. Deze hackers kraken wachtwoorden op bestelling, verzorgen cryptografische bescherming, schrijven malware, versturen spam en bouwen of verhuren botnets.

Arena en zijn collega's houden de activiteiten van deze criminelen in de gaten en verkopen hun inzichten door aan grote banken, die vaak slachtoffer zijn van hun hacks. Die kunnen dan tijdig maatregelen nemen.

Waarom dit allemaal zo makkelijk gaat

Langzaam maar zeker is het ons duidelijk. Onze persoonlijke data lopen grote risico's om te worden gehackt en gestolen, door partijen en op manieren die ons grote schade kunnen toebrengen. Dit wisten we natuurlijk al wel. Het nieuwe inzicht is dat dit geen incidentele, maar structurele, systemische risico's zijn. Waar komt deze fundamentele onveiligheid vandaan?

De Amerikaanse cryptograaf Bruce Schneier kan deze vraag als geen ander beantwoorden. In talloze lezingen, columns en boeken probeert hij de problemen rondom online veiligheid te doorgronden en uit te leggen. Uit zijn omvangrijke oeuvre destilleren we drie lessen die ons helpen de ware aard van online veiligheid te begrijpen.[28]

Allereerst: er bestaat een groot verschil tussen de veiligheid van fysieke producten en online producten. Dat verschil zit volgens Schneier vooral in het ontwerpproces. Hij stelt dat er twee manieren zijn om producten te beveiligen. Ten eerste door een product zo goed mogelijk te beveiligen voordat het de markt opgaat. Een auto gaat niet de weg op voordat die uitvoerig getest is. Een vliegtuig moet aan vele eisen voldoen, voordat de eerste vlucht plaatsvindt. Ten tweede kan een product beveiligd worden terwijl het al op de markt is en gebruikt wordt. Dit is bij software vaak het geval: die bevat mankementen die gaandeweg, met behulp van security-updates, verholpen worden. Iedereen die weleens met een Windowscomputer werkt, merkt geregeld dat de computer allerlei software moet downloaden en installeren. Dan worden onder andere veiligheidslekken gedicht. Een groot deel van onze internettechnologie wordt op die manier ontworpen: rommelig, ad hoc, stukje bij beetje. Dat geeft de risico's die onze data lopen een fundamenteel karakter: er zitten altijd, maar dan ook echt altijd, tekortkomingen in de beveiliging van onze (digitale) gegevens.

De tweede les van Schneier is dat de beveiliging van technologieën en onze data altijd de uitkomst is van botsende belangen. We willen niet dat een hacker een auto op afstand kan stilzetten, maar misschien wel dat de politie dat kan. We willen bedrijfsinformatie graag binnenskamers houden, maar ook thuis kunnen werken.

Dit geldt voor veel bedrijven die hun kortetermijnbelang – geld verdienen – laten prevaleren boven de noodzakelijke investeringen voor een goede beveiliging – hun langetermijnbelang. Deze bot-

sing van belangen is vooral goed te zien bij overheden. Enerzijds moeten zij er zorg voor dragen dat de rechten van hun burgers ook online gewaarborgd worden. Aan de andere kant willen met name opsporings- en veiligheidsdiensten juist gebruik kunnen maken van zwakheden binnen de apparaten en netwerken van burgers, om zo toegang te krijgen tot informatie. Deze wens leidt geregeld tot conflicten.

Zo vlogen in 2016 de FBI en Apple elkaar publiekelijk in de haren. De Amerikaanse opsporingsdienst wilde dat Apple software schreef om daarmee de beveiliging van de iPhone 5 van een omgekomen terrorist te omzeilen. CEO Tim Cook weigerde dat. Volgens de Applebaas was het FBI-verzoek niets minder dan een poging om een permanente achterdeur in te bouwen. Met zo'n achterdeur zouden opsporings- en veiligheidsdiensten altijd bij de gegevens in dat type iPhone kunnen. De FBI koos uiteindelijk voor een andere oplossing: de dienst vond een bedrijf dat de telefoon van de terrorist wist te hacken.

Het gevecht tussen Apple en de FBI staat voor een groter conflict dat al tientallen jaren woedt tussen opsporings- en veiligheidsdiensten en technologiebedrijven. Deze strijd wordt ook wel de Crypto War genoemd; hij begon eind jaren tachtig met een strijd over cryptografie.[29] Tot dan toe was sterke cryptografie een zaak van inlichtingendiensten die hun berichten ermee beveiligden of berichten van anderen probeerden te kraken. Met de opkomst van internet werd cryptografie ook belangrijk voor technologiebedrijven. Mailproviders wilden voorkomen dat onbevoegden mee konden lezen in het mailverkeer. Webwinkels en financiële instellingen wilden hun betalingsverkeer versleutelen om diefstal te voorkomen. Overheden en geheime diensten verzetten zich hier lang tegen. Het maakte hun werk stukken ingewikkelder. Eind jaren negentig moesten ze dat verzet opgeven: het internet groeide simpelweg te hard en de risico's werden te groot voor gebruikers om geen cryptografie te gebruiken. Maar nog steeds is met iedere nieuwe technologische dienst de vraag bij opsporings- en veilig-

heidsdiensten: kunnen wij nog wel in de apparaten komen? En als ze die kwetsbaarheid niet goedschiks in de technologie kunnen bouwen, dan kwaadschiks. Door de onthullingen van Edward Snowden weten we dat de NSA opzettelijk cryptografische standaarden heeft verzwakt, apparatuur, bedoeld voor de export, heeft onderschept om afluisterapparatuur in te bouwen, bedrijven heeft gehackt en nog veel meer.

Met andere woorden: naast de bescherming van de data van burgers, zijn overheden er ook bij gebaat als de beveiliging van die data kwetsbaarheden heeft. Waardoor de data van burgers structureel gevaar lopen. Want wat een kwetsbaarheid is voor de NSA, kan óók een kwetsbaarheid zijn voor de Russische geheime dienst of voor een hacker. Zoals Schneier geregeld zegt: 'NSA's geheimen van nu zijn het PhD-onderzoek van morgen en de hackertrucs van overmorgen.' Als je een achterdeur installeert, kun je nooit voorkomen dat andere partijen die ook ontdekken en misbruiken. Een ironisch voorbeeld: in 2015 hackten een aantal Amerikaanse academici de site van de NSA. Zij maakten daarbij gebruik van een kwetsbaarheid in de encryptie. Die kwetsbaarheid was jaren eerder op last van de NSA zelf aangebracht in deze vorm van encryptie, maar alleen bedoeld voor software die naar het buitenland geëxporteerd zou worden. Op de een of andere manier was die software op de servers van de NSA terechtgekomen. Door de NSA zelf.

Schneiers derde les over de systemische onveiligheid van onze digitale data is dat de aanvaller sterker staat dan de verdediger. De aanvaller hoeft maar één zwakte in de verdediging te vinden om binnen te komen, terwijl de verdediger heel veel ingangen moet verdedigen om de aanvaller buiten te houden. Zo legde in 2015 een aantal Russische hackers, vermoedelijk in opdracht van het Kremlin, Oekraïense elektriciteitscentrales plat. Stal een hacker in 2014 en 2015 alle data van twee surveillancebedrijven – Gamma International en Hacking Team –, waarna die bedrijven bijna failliet gingen. En kon een tiener in het voorjaar van 2016 inbreken op het privé-e-mailaccount van zo ongeveer de laatste persoon van

wie je het verwacht: de baas van de CIA. Niet alleen is de schade soms heel groot, deze voorbeelden laten ook zien dat er vaak maar weinig mensen nodig zijn om veel schade aan te richten.

Wij zijn zelf ook verantwoordelijk

Dat internettechnologie fundamentele risico's met zich meebrengt, heeft overduidelijk consequenties voor de persoonlijke data van de gewone gebruiker. Maar laten we die gebruiker zelf ook niet uitvlakken. Als het niet bedrijven zijn die falen in hun internetbeveiliging, of overheden die opzettelijk software en infrastructuur verzwakken, of hackers die een kier weten te vinden in apparaten of systemen, dan zijn wij er altijd zelf nog: feilbare en onwetende gebruikers. Technologie kan nog zo goed en veilig ontworpen zijn, tegen menselijke fouten en slechte beveiliging is geen systeem opgewassen.

Wij kiezen de simpelste wachtwoorden, installeren de laatste beveiligingsupdates niet of veel te laat, zetten onze intiemste documenten onbeschermd op ons bureaublad, mailen onze inlogcodes rond en vergeten zelfs de basaalste beveiligingsmaatregelen te nemen. Illustratief voor deze laksheid is de rondgang die wij in 2014 maakten langs een aantal copyshops in Amsterdam, Groningen en Rotterdam. Het enige wat wij deden was kijken op het bureaublad van de computers waarvandaan klanten printopdrachten geven. Wat wij bevroedden bleek waar: heel vaak vergaten klanten het document van de copyshopcomputer te verwijderen. Zo verzamelden we in korte tijd contracten, foto's, rekeningoverzichten, een brief van een weduwe over de erfenis aan de Belastingdienst, de complete klassenlijst van een middelbare school met alle namen, geboortedata en e-mailadressen van de kinderen en boekingsinformatie voor een reis naar Turkije.[30]

Toegegeven: altijd op je hoede zijn is ook om gek van te worden. Als je na moet denken bij elke digitale stap die je zet, ieder stukje data dat je achterlaat, elke online dienst waar je gebruik van maakt, dan houd je geen leven over. Aan de andere kant maakt een ruime meerderheid van ons zich grote zorgen over de veiligheid van onze digitale data. 57 procent van de Europeanen vreest dat zijn persoonlijke informatie niet veilig is.[31] 77 procent van de internetgebruikers zegt bang te zijn voor diefstal van online data.[32] Logisch ook, gezien de bijna dagelijkse berichtgeving over spectaculaire datadiefstallen en hackende geheime diensten.

Minder vanzelfsprekend is dat we toch op dezelfde, onveilige voet verdergaan. Ook wat betreft de beveiliging van onze apparaten en systemen lijkt de privacyparadox te gelden: wij zeggen privacy belangrijk te vinden, maar gedragen ons er niet naar. Als het ons gevraagd wordt, geven wij aan geen vertrouwen te hebben in de veiligheid van onze data, tegelijkertijd handelen wij niet naar die zorgen.

We ervaren de onveiligheid niet

Hoe kan dat? Waarom gebruiken wij de digitale systemen en diensten uiteindelijk toch, terwijl wij weten dat er genoeg reden is om ze niet te vertrouwen? We nemen contact op met Esther Keymolen, een Belgische techniekfilosofe die in april 2016 promoveerde op online vertrouwen.

Met online vertrouwen is iets bijzonders aan de hand, legt Keymolen uit. Als wij gebruikmaken van een online dienst of digitale technologie, dan ervaren wij slechts één onderdeel ervan: het gebruikersniveau. 'We zien de interface en dat is het,' stelt Keymolen. 'Ik vertrouw mijn telefoon, mijn beveiligingscamera en mijn apps omdat ze doen wat ik verwacht dat ze doen. Onze beoordeling gaat vaak niet verder dan: werkt het of werkt het niet?'

Het probleem is, zegt Keymolen, dat de ervaring daar stopt. 'Wij ervaren niet hoe de technologie echt werkt en welke gevolgen dat heeft. Mensen ervaren niet dat er meegekeken kan worden met hun camera. De meeste gebruikers – uitzonderingen daargelaten – ervaren niet dat hun gegevens gestolen kunnen worden of dat ze gebruikt kunnen worden voor identiteitsfraude. Daardoor wordt ons vertrouwen nooit echt getest en is het lastig om te beoordelen of het vertrouwen wel terecht is.'

Beveiliging gaat eigenlijk over twee dingen, vervolgt de filosofe. 'Over het buiten houden van vreemden én het binnen houden van bepaalde gegevens. Diensten en technologieën willen hackers en overheden buiten houden en vertrouwelijke gegevens niet verliezen. Maar als je kijkt naar veel van de digitale technologieën, dan zijn die er ook op gericht om het makkelijk te maken om gegevens te verzamelen, op te slaan en uit te wisselen. En ze moeten ook makkelijk te bedienen zijn voor de gebruiker. Zoals gezegd: in de ervaring is er vertrouwen, want het werkt. Maar wij kunnen de beveiliging niet beoordelen. Hoe onze data worden beschermd en de buitenwereld wordt afgeschermd, ervaren wij niet. Het is een black box, waar de gemiddelde gebruiker niet in komt.'

Dat verklaart ook waarom wij zeggen dat wij apparaten en online technologieën niet vertrouwen, maar ons daar niet naar gedragen. 'Als je erover nadenkt omdat je ernaar gevraagd wordt, ben je wantrouwend. Maar als je het gebruikt, verdwijnt dat naar de achtergrond omdat je de partij, de technologie en de risico's erachter niet ziet.'

Dus? 'Zelf de beveiliging verhogen is voor bijna niemand een serieuze optie,' zegt Keymolen. 'Je hoort ook weleens: dan moet je het maar niet meer gebruiken. Maar dat is natuurlijk geen echte keuze meer. Ons leven is zo vervlecht geraakt met die technologieën, dat we echt niet meer zonder kunnen.'

Wat ons rest is vasthouden aan wat we al hebben: een naïef vertrouwen in de diensten en producten die wij gebruiken. En: erop vertrouwen dat wij geen slachtoffer zullen zijn van de lange arm van de geheime diensten of de volgende onvermijdelijke hack.

'Het verzamelen van steeds meer informatie en het aanleggen van koppelingen daartussen lijkt nauwelijks meer in het gareel te krijgen. Het resultaat is dat informatie vervuilt, onduidelijk is wie verantwoordelijk is voor informatiestromen en dat burgers, bedrijven en ook instanties binnen de overheid zelf, verst(r)ikt raken in de datakluwen van de overheid.'[33]

– WETENSCHAPPELIJKE RAAD VOOR HET REGERINGSBELEID

'Iemand moest Josef K. belasterd hebben, want zonder dat hij iets kwaads had gedaan, werd hij op een morgen gearresteerd.'[34]

– SCHRIJVER FRANZ KAFKA

3

Google en de Belastingdienst

Hoe de grote datagraaiers onze gegevens in hun greep hebben

In juni 2012 meldt de 36-jarige Rus Alexander Dolmatov zich bij een Nederlands asielzoekerscentrum. Dolmatov is in zijn moederland gearresteerd bij een demonstratie tegen president Vladimir Poetin. Hij vreest voor zijn leven. In december 2012 bepaalt de Immigratie- en Naturalisatiedienst (IND) dat de asielzoeker niet in Nederland mag blijven. Dolmatovs advocaat gaat in beroep. Alleen: INDiGO, het systeem dat de IND gebruikt, registreert dit niet. Het vakje dat in dit geval moet worden aangevinkt, werkt niet. Volgens INDiGO is Dolmatov 'verwijderbaar.'

Een paar weken later bellen medewerkers van het asielzoekerscentrum de politie. Dolmatov is dronken, verward en suïcidaal. De agenten brengen hem naar een opvanglocatie in Dordrecht. Hierna wordt Dolmatov overgebracht naar Detentiecentrum Rotterdam om te worden uitgezet. Zijn advocaat wordt niet ingelicht.

Vier dagen daarna vinden medewerkers Dolmatov dood in zijn cel. Zelfmoord. Een onderzoekscommissie van de Inspectie Veiligheid en Justitie velt een paar maanden later een hard oordeel over de zaak-Dolmatov. De overheid heeft volgens de commissie onzorgvuldig gehandeld. '[Dat] is niet alleen toe te schrijven aan het handelen of nalaten van functionarissen, maar ook aan de afhankelijkheid van – en het vertrouwen in – de systemen, procedures en formulieren die functionarissen bij hun besluiten in die keten ondersteunen,' schrijft de Inspectie. 'Het is de Inspectie gebleken dat de systemen, procedures en formulieren in de praktijk te vaak summiere, onduidelijke en soms

zelfs onjuiste informatie bevatten en dat ze onderling onvoldoende accuraat en actueel op elkaar aansluiten. Het is zorgelijk te signaleren dat deze systeemomissies voor een belangrijk deel bekend zijn.'[35]

Alle overheidsdata over burgers in kaart brengen

Ruim twee jaar later zitten wij met een man of twintig in de tuin van de redactie van *De Correspondent*. Met hackers, juristen, ambtenaren en journalisten proberen we een ambitieus plan ten uitvoer te brengen. We willen in één dag alle datastromen binnen de Nederlandse Rijksoverheid in kaart brengen.

In de zonovergoten tuin schuift ook Douwe Schmidt aan. Schmidt noemt zichzelf 'datamijnwerker' en houdt voor *De Correspondent* een 'datadagboek' bij. Hierin beschrijft hij zijn moeizame en soms hilarische zoektocht naar zijn opgeslagen data bij overheden en bedrijven. Hij probeert bijvoorbeeld uit te vinden welke gegevens zijn gemeente, Amsterdam, aan kerken heeft verstrekt. Zijn doel is om een beeld te krijgen van zijn 'digitale alter ego', dat verspreid over honderden databases ligt opgeslagen. Wie kan bij zijn data? Wat vertellen die data over hem?

Zijn wapen is artikel 35 van de Wet bescherming persoonsgegevens. Daarin staat dat iedere Nederlandse burger het recht heeft om bij overheden en bedrijven te vragen of zij persoonsgegevens van hem verwerken en, indien dat het geval is, daar een volledig overzicht van te ontvangen.

Schmidt krijgt vooral onbevredigende antwoorden. Terwijl de zon langzaam ondergaat, concludeert hij: 'Ik zal nooit te weten komen waar mijn data liggen, met wie die data worden gedeeld en wie er toegang tot heeft.'

Alle aanwezige hackers, juristen, ambtenaren en journalisten zijn even stil. Dan zegt een ambtenaar die verantwoordelijk is voor het databeheer van een van de grootste Nederlandse gemeenten: 'Ja, dat

klopt. Maar wat dacht je van mij? Voor mij is het óók onmogelijk om achter te komen welke data van jou waar bij ons liggen opgeslagen.'

De ambtenaar legt uit dat niemand in zijn gemeente het overzicht heeft over alle datastromen. Er is geen centraal loket waar alle data zijn op te vragen. Hij zou het graag willen hoor, juist daarom is hij hier. Maar waar te beginnen?

De hackers, datajournalisten en nerds kruipen weer achter hun laptop. De hele dag al proberen we met elkaar enkele gigabytes aan overheidsdata in het gareel te slaan. De kunst is om te ontdekken welke overheidsinstanties onderling persoonlijke data van burgers uitwisselen en om welke data dat gaat.

Een maand eerder plaatsten we een oproep op *De Correspondent*. Wie wilde ons komen helpen alle datastromen van de Nederlandse Rijksoverheid in kaart te brengen? Enkele technisch begaafden en experts zegden hun medewerking toe.

Ter voorbereiding zochten we op vage overheidswebsites naar overzichten van databases, convenanten over de uitwisseling van informatie tussen overheidsdiensten, evaluaties van het gebruik van het burgerservicenummer door publieke en private partijen, wiki's over basisadministraties en nog veel, veel meer.

Een paar weken eerder kregen we ook het Meldingenregister van de privacytoezichthouder Autoriteit Persoonsgegevens in ons bezit. Overheden en bedrijven die structureel persoonsgegevens verwerken, moeten in dit register melden welke gegevens ze verwerken, wat het doel is van die verwerking, wat er met die persoonsgegevens gebeurt, wie er verantwoordelijk is en, vandaag voor ons heel interessant, met wie die gegevens worden gedeeld. Ons doel is van deze totaal verschillende databronnen een overzicht maken. De directe aanleiding van deze exercitie vormt een ambitieus plan van de minister van Veiligheid en Justitie. En een Excelbestand.

In december 2014 presenteert het ministerie van Veiligheid en Justitie een plan voor de kaderwet gegevensuitwisseling.[36] Voor-

alsnog is die alleen van toepassing op fraudebestrijding, maar de werkgroep die de plannen uitwerkt stelt dat deze nieuwe wet ook moet gelden voor de bestrijding van andere vormen van criminaliteit.

Als het voorstel inderdaad een wet wordt, maakt het de grootschalige uitwisseling mogelijk van gegevens tussen overheidsdiensten, gemeenten en private partijen die ook in de fraudebestrijding actief zijn. Er bestaan al enorm veel mogelijkheden om gegevens uit te wisselen, maar blijkbaar niet genoeg: met de voorgestelde plannen wordt een aantal juridische obstakels uit de weg geruimd waardoor er minder aan de wet getoetst hoeft te worden.

De Tweede Kamer is niet meteen overtuigd van de noodzaak van het plan. Kan de minister niet eerst vertellen welke informatie al binnen de overheid gedeeld wordt? Minister van Veiligheid en Justitie Ard van der Steur zet een aantal ambtenaren aan het werk. In april 2015 verschijnt een tussenrapportage: het in kaart brengen van de informatiestromen binnen de Rijksoverheid blijkt moeilijker dan gedacht, schrijft de minister. Wel is alvast een Excelbestand bijgevoegd, met daarin een overzicht van de koppelingen van databestanden. Het is een onleesbare brij van namen, systemen en ministeries die met kruisjes en strepen verbonden zijn.

Ondanks het chaotische Excelbestand zijn we enthousiast over Van der Steurs initiatief om al die koppelingen eens in kaart te brengen. Een van de grondslagen van het privacyrecht is immers dat iedere burger het recht heeft om te weten welke informatie van hem waar ligt opgeslagen en wat daarmee gebeurt – precies het recht waar Douwe Schmidt aanspraak op wilde maken. Dat de Nederlandse overheid – de grootste Nederlandse verzamelaar van persoonlijke informatie – een belangrijke stap zet in het openbaren van het overzicht van huidige bestandskoppelingen, valt alleen maar toe te juichen. En we helpen graag mee het bestand te verfijnen. Na onze onderzoeken naar de datastromen die onze apps en veelbezochte websites verzamelen en de analyse van de fundamentele onveiligheid van de systemen en sites waar wij onze data

aan toevertrouwen, is dit een logische stap in onze zoektocht. We zijn benieuwd naar de manier waarop de Nederlandse overheid met de gegevens van haar burgers omgaat.

Niemand heeft het overzicht

Maar eerst: wat heeft de dood van Alexander Dolmatov te maken met onze poging om de datakluwen van de overheid te ontwarren? Het antwoord schuilt in een invloedrijk rapport van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) dat in 2011 verscheen: *iOverheid*.[37] De auteurs van *iOverheid* beschrijven hoe door digitalisering en informatisering de Nederlandse overheid stilzwijgend van een zogenoemde 'e-Overheid' in een 'iOverheid' is veranderd. Een verschuiving die de relatie tussen overheid en burger grondig heeft veranderd en de rem van de verzameling en het gebruik van de persoonlijke informatie van burgers heeft gehaald.

Een e-Overheid is een overheid die ICT gebruikt om haar burgers van dienst te zijn. Je kunt met een DigiD online aanspraak maken op allerlei voorzieningen, vergunningen aanvragen en je belastingen aangeven. Ook zijn er tientallen databases en applicaties opgezet die maatschappelijke problemen moeten helpen voorkomen of verminderen. Denk aan het Elektronisch Kind Dossier, dat tegenwoordig Digitaal Dossier Jeugdgezondheidszorg heet. Hierin wordt informatie verzameld over alle gezinnen met als doel problemen bij kinderen vroeg te signaleren. Of denk aan de Verwijsindex, een systeem waarin meldingen van mogelijke kindermishandeling en -misbruik bij elkaar komen zodat hulpverleners niet meer langs elkaar heen werken en belangrijke informatie met elkaar delen. Ook is er Suwinet, waarmee verschillende overheidsdiensten informatie uitwisselen over uitkeringsgerechtigden, om zo te bepalen of iemand recht heeft

op een uitkering. Fraude met sociale voorzieningen wordt opgespoord met SyRI, een systeem waarin per uitkeringsgerechtigde het risico op fraude wordt berekend.

Telkens als de e-Overheid een dergelijke database of applicatie optuigt, is er een debat over in de Tweede Kamer. Geregeld gaat daar een publieke discussie in de media aan vooraf. Wordt de privacy van de burgers wel genoeg beschermd? Toezichthouders en adviesorganen toetsen vervolgens de noodzaak van zo'n systeem en na wat aanpassingen wordt er dan vrijwel altijd groen licht gegeven.

Waar niet naar wordt gekeken, zo stellen de auteurs van het WRR-rapport, is de *samenhang* tussen al deze systemen. Veel van de losse databases en systemen van de overheid blijken *aan elkaar gekoppeld* te zijn. Informatie ligt niet *opgeslagen* in al die databases, nee, die informatie *stroomt* van de ene database naar de andere, van het ene overheidsorgaan naar het volgende. Ziedaar de iOverheid. Het voorstel uit 2014 van minister Van der Steur om nog meer databases aan elkaar te koppelen, is te zien als een ultieme uiting hiervan.

Een goede illustratie van de iOverheid is de Haagse Pandbrigade, een ambtelijk team dat zogenoemde risicohuizen bezoekt in de Hofstad. Dit zijn huizen waarin zich mogelijk allerlei problemen afspelen, van illegale bewoning tot verloedering en van overlast tot criminaliteit. Als twee niet-gehuwde personen op één adres staan ingeschreven, kan dat een reden voor bezoek zijn, want mogelijk is daar sprake van illegale onderhuur. Eenmaal binnen letten de inspecteurs niet alleen op illegale bewoning, maar kijken ze ook of de leerplicht wordt nageleefd als er kinderen zijn, of er sprake is van een risicovolle gezinssituatie en of er schulden zijn bij de bewoners. Die informatie kan vervolgens gedeeld worden met de Haagse politie, de leerplichtambtenaar, regionale overlegorganen, de GGD, de gemeente en jeugdzorg.

Dit Haagse voorbeeld staat niet op zich. Omdat steeds meer instanties samenwerken aan een 'integrale aanpak' van allerlei sociale problemen, stroomt er ook meer informatie rond. We moeten de digitale overheid daarom niet meer zien als een verzameling losse databases en applicaties, maar als een verzameling informatiestromen. 'Stapje voor stapje,' schrijft de WRR, ontstaat er 'een kluwen van datastromen. Op Rijksniveau. Op lokaal en uitvoeringsniveau. En zeker ook op het internationale en Europese niveau.'

Hierdoor is er een groot probleem ontstaan, constateren de auteurs. Niemand heeft meer het overzicht over al die stromen, laat staan dat iemand er de regie over voert. Voor de burger betekent dit: je kunt er niet van uitgaan dat jouw informatie bij de instantie blijft waaraan je die hebt gegeven. Dus: wie kun je nog aanspreken als er iets misgaat met die informatie? Stel dat de Haagse Pandbrigadier onterecht vaststelt dat je niet aan de leerplicht voldoet. Wie corrigeert die informatie dan?

Een van de belangrijke lessen van *iOverheid* is dat politici zich niet realiseren dat de e-Overheid in een iOverheid is veranderd. Er is sprake van een heilig geloof in het optuigen van nieuwe databestanden en databases. Voor meer veiligheid, meer efficiëntie, meer effectiviteit. De iOverheid, stellen de auteurs, kent door dit 'politiek enthousiasme' geen natuurlijke grenzen. De dataspaghetti – al die stromen en verbonden databases – zal blijven groeien, gevoed door de data van Nederlandse burgers.

De verontrustende consequentie daarvan is dat fundamentele beginselen hier de dupe van zijn. Door het primaat bij de technologie te leggen, komen essentiële waarden in de knel. Zoals privacy. In de woorden van de WRR: 'Het politieke enthousiasme voor nieuwe applicaties en koppelingen van systemen en informatiestromen gaat hand in hand met argumenten als het vergroten van de veiligheid en verhogen van effectiviteit en efficiëntie. Deze waarden zorgen, gecombineerd met het probleemoplossende 'imago' van ICT, als het ware voor zichzelf: per maatregel (een systeem, een koppeling) blijken ze in de regel zwaarder te wegen dan waarden als transparantie, privacy, keuzevrijheid of accountability.'

Hoe de grootste overheidsdatabank met onze gegevens omgaat

Als we de informatiekluwen van de overheid willen doorgronden, ontkomen we niet aan de Belastingdienst. Om zijn taken uit te voeren – belastingen heffen en innen, toeslagen uitkeren, belastingfraude bestrijden – heeft de Belastingdienst bakken data nodig. Ga maar na: om alleen al te kunnen controleren of iemand recht heeft op huurtoeslag, moet de Belastingdienst niet alleen de huurprijs van het huis kennen en weten wat diegene verdient, maar ook wat zijn medehuurder verdient, of de persoon wel staat ingeschreven op het opgegeven adres, wie daar nog meer staat ingeschreven, of de persoon eigen vermogen heeft en of de persoon niet ergens anders een koophuis heeft, et cetera. En dit is nog een relatief simpel voorbeeld.

Wij zijn benieuwd hoe de grootste uitvoerende overheidsdienst met al die data omgaat. Hoe komt de dienst aan onze gegevens? En wat wordt ermee gedaan?

Een goed startpunt van ons onderzoek is hoogleraar Recht en Informatiemaatschappij én privacyadvocaat Gerrit-Jan Zwenne. In 1998 promoveerde Zwenne op de vraag welke informatie de Belastingdienst over burgers kan verzamelen. 'Ik kwam al vrij snel tot de conclusie dat je die vraag eigenlijk om zou moeten draaien,' vertelt Zwenne in zijn Haagse werkkamer. 'Wat kan de Belastingdienst niet? En sinds mijn promoveren is de wetgeving alleen maar verruimd.'

Dat is de Belastingdienst niet te verwijten, vindt hij. De fiscus is een uitvoerder van politieke beslissingen. 'Een belastinginspecteur mag volgens de wet gegevens opvragen als die 'fiscaal relevant' zijn, maar we hebben in Nederland ongeveer alles fiscaal relevant gemaakt. Onze belastingwetgeving is zo uitgebreid, ingewikkeld en genuanceerd, dat de Belastingdienst wel heel gedetailleerd moet gaan kijken naar de persoonlijke omstandigheden van de belastingbetaler. Een haast onvermijdelijk gevolg is dat de Belastingdienst grote sleepnetten moet uitgooien om informatie te vergaren.'

Eind 2013 kwam zo'n sleepnet aan het licht toen bleek dat de Belastingdienst alle transacties van alle klanten van SMSParking had opgevraagd, een bedrijf waar automobilisten met hun mobiele telefoon voor een parkeerplaats kunnen betalen. Zo kon de Belastingdienst zien waar en wanneer leaseautorijders hun auto parkeerden en of zij zich wel aan het aantal toegestane privékilometers hielden. Het letterlijke verzoek aan SMSParking luidde: 'Ik verzoek u alle parkeergegevens (kenteken, datum, plaats (locatie) en tijd) van uw cliënten over het jaar 2012 aan mij te verstrekken. De Belastingdienst zal deze gegevens gebruiken ten behoeve van de motorrijtuigenbelasting, de belasting van personenauto's en motorrijwielen 1992 (BPM), de belasting zware motorrijtuigen, de inkomstenbelasting, de loonbelasting, de vennootschapsbelasting en de omzetbelasting.'[38]

De fiscus vroeg dus niet gericht naar data van één specifiek individu, maar vroeg ineens de gegevens op van *alle* klanten van dit bedrijf, voor *meerdere* doeleinden.

De eigenaar van SMSParking weigerde. Hij wilde de privacy van zijn klanten beschermen. Daarop stapte de fiscus naar de rechter. Die kwam eind november 2013 met een glasheldere uitspraak: de Belastingdienst was inderdaad te ver gegaan en zijn verzoek schond het recht op privacy, zoals beschreven in het Europees Verdrag voor de Rechten van de Mens. De rechter sprak over een '*fishing expedition*' van de Belastingdienst, een uitgezet sleepnet in de hoop dat er iets interessants tussen zat. Dat botste volgens de rechter met het principe van een gezonde verhouding tussen burger en overheid. De rechter: 'Het dagelijks doen en laten van de burgers gaat de overheid niets aan.'

De Belastingdienst ging meteen in hoger beroep en met succes: SMSParking moest de gegevens alsnog afstaan. De hogerberoepsrechter maakte korte metten met de woorden van zijn collega. Ook

het argument dat de Belastingdienst een specifiekere aanvraag bij SMSParking had kunnen doen, door bijvoorbeeld alleen reeds verdachte kentekens op te vragen, werd van tafel geveegd. De rechter vatte de onaantastbaarheid van de fiscus samen met de woorden: 'Daarbij is het niet van belang of de Belastingdienst ten tijde van het opvragen dan wel raadplegen van inlichtingen en gegevens bij een administratieplichtige ten behoeve van belastingheffing van derden nog niet weet of die inlichtingen en gegevens van belang zijn voor de belastingheffing bij een bepaalde belastingplichtige.'

Met andere woorden: de rechter gaf de fiscus de ruimte om te blijven vissen. Met sleepnet.

Later bleek dat andere parkeerbedrijven, in tegenstelling tot de dappere eigenaar van SMSParking, wél klakkeloos akkoord zijn gegaan met het verzoek. Dat betekent dat de fiscus van duizenden Nederlandse automobilisten exact weet, voor een periode van ten minste een jaar waar, wanneer en hoelang zij parkeerden. Op welk adres zij lunchten, bijvoorbeeld. Of waar zij de nacht doorbrachten. En let wel: we zijn hier alleen van op de hoogte omdat SMS-Parking bereid was om naar de rechter te stappen.

Een ander voorbeeld van de ondoorzichtigheid bij de fiscus. In 2012 kreeg een automobiliste een naheffing en een boete van de Belastingdienst. Ze kon niet aantonen dat ze jaarlijks minder dan 500 kilometer in een auto van de zaak had gereden, zoals maximaal is toegestaan buiten werktijd. De fiscus concludeerde na eigen onderzoek dat ze dus méér moest hebben gereden.

Hoe kwam de Belastingdienst aan die informatie?

Haar advocaten Guido de Bont en Annabel Vissers moesten een beroep doen op de Wet openbaarheid van bestuur om een antwoord te krijgen op die vraag. En kwamen erachter dat de Belastingdienst en het Korps landelijke politiediensten, tegenwoordig onderdeel van de Nationale Politie, een convenant hebben gesloten. Daarin is vastgelegd dat de fiscus iedere vrijdag een kopie van de politie krijgt van alle kentekenregistraties die de ruim tweehonderd mobiele en vaste politiecamera's op de Nederlandse snelwegen maken.

Dat betekent: foto's van alle auto's die op de Nederlandse snelwegen rijden.

Terwijl de politie de plicht heeft die registraties binnen 24 uur te verwijderen. Alleen als een van de kentekens een zogenoemde *hit* geeft en op naam staat van een persoon die door de politie wordt gezocht of een boete open heeft staan, mag de informatie over dat kenteken bewaard blijven. Maar de Belastingdienst, zo blijkt uit het convenant, ontvangt het hele jaar door alle kentekenregistraties van een hele week, ook de no-hits, op een 'beveiligde disk' die door een 'gecertificeerd koeriersbedrijf' wordt gebracht.

En een kenteken lijkt misschien onpersoonlijk, maar kan veel onthullen. Dergelijke registraties geven een gedetailleerd beeld van het gedrag van miljoenen Nederlanders. Waar iemand werkt, hoelang iemand onderweg is, of iemand elke dinsdagmiddag bij een Van der Valkhotel parkeert, allerlei zeer persoonlijke zaken kunnen ervan worden afgeleid. Precies de reden dat de politie die gegevens één dag mag bewaren. Volgens de Nederlandse belastingwet daarentegen mag de fiscus de gegevens zo lang bewaren als 'fiscaal relevant' is. Dat betekent: alle kentekenregistraties van auto's op de Nederlandse snelwegen die door de Belastingdienst als 'fiscaal relevant' worden beschouwd, worden door de fiscus vijf tot zeven jaar bewaard. De wettelijke waarborgen die de politie verhinderen om buitensporig veel persoonsgegevens te verzamelen, gelden niet voor de Belastingdienst.

Een wettelijke achterdeur

We besluiten ons verder te verdiepen in de dienst en ontdekken dat de Belastingdienst niet alleen maar datastromen naar binnen hengelt voor eigen gebruik: de fiscus is ook leverancier van data aan andere overheidsinstellingen. De Belastingdienst heeft een

geheimhoudingsplicht. Mag dus gegevens over Nederlandse burgers niet met andere partijen delen. In de belastingwet lezen we dat er *uitzonderingen* bestaan op deze geheimhoudingsplicht. Onder 'bepaalde voorwaarden' mogen andere overheidsdiensten wél gegevens bij de fiscus opvragen. Onder andere de AIVD, de MIVD en de officier van justitie kunnen zo toegang krijgen tot de datagoudmijnen van de fiscus. Die, zo leerden we, niet alleen uit de gegevens van miljoenen Nederlanders over werk-, loon- en banktransacties bestaan, maar daar kunnen ook kentekenregistraties, parkeergedrag en reisgedrag in het openbaar vervoer tussen staan.

In een artikel dat we in september 2014 op *De Correspondent* publiceren, betitelen we deze mogelijkheid als een 'wettelijke achterdeur.' Het gaat immers om data die andere overheidsdiensten niet zelf mogen vorderen of minder lang mogen bewaren.[39]

Het verhaal wordt opgepikt door andere media. Het is een mooie scoop, waar zelfs meerdere Kamervragen over worden gesteld. Hoewel, scoop? Dit staat gewoon in een wet. Toch is het feit dat dit zo breed wordt opgepikt, dat er zoveel ophef over komt en dat zelfs enkele hoogleraren – 'deze achterdeur staat wagenwijd open,' zei emeritus hoogleraar strafrecht Theo de Roos verbaasd – en privacyadvocaten die wij het voorlegden er niet van op de hoogte blijken veelzeggend. Wetten die de burger tegen de staat moeten beschermen, zijn even ondoorzichtig als de privacyvoorwaarden van sites en apps die wij eerder bespraken: kleine lettertjes die niemand allemaal leest.

Hoe kun je bij zo'n hongerige overheidsdienst de privacy van miljoenen Nederlanders waarborgen? We maken in april 2015 een afspraak met Hans Blokpoel, de directeur van de Belastingdienst. In het gesprek beaamt hij dat de fiscus zijn eigen weg volgt. Op onze opmerking dat hij verplicht is om de persoonlijke data die zijn organisatie verwerkt aan te melden bij de Autoriteit Persoonsgegevens, antwoordt de topambtenaar: 'Ik vind het vrijwel altijd logisch om dat soort dingen te melden. Maar er zijn ook situaties waarbij

ik zeg: sorry, in dit geval weegt de opsporing of fraudebestrijding zo zwaar, dat ik mijn modus operandi niet kan blootgeven.'

Blokpoel doet nog een opvallende bekentenis. Hij vertelt ons dat zijn dienst gestopt is met het opvragen van parkeergegevens bij bedrijven – de kwestie die had geleid tot de rechtszaken. 'Dit was voor mij persoonlijk ook over de grens.' Blokpoel heeft het programma stilgezet, zo zegt hij, omdat hij deze bulkverzameling 'niet-proportioneel' vond. Hij deed dat pas nádat die gegevens niet zo nuttig bleken. 'Wij hebben gekeken wat deze gegevens nu aan extra informatie opleverden. Als dan de conclusie is dat het eigenlijk niet heel veel oplevert, dan is het niet proportioneel en vind ik dus dat de dienst een natuurlijke terughoudendheid moet hebben.'

Kafka in de polder

Waarom zo moeilijk doen over rondstromende data bij de overheid? Inspecties kunnen nu beter controleren. Hulpverleners kunnen beter samenwerken. Politieagenten kunnen zich een beter beeld vormen van een verdachte. AIVD'ers kunnen sneller naar terroristen zoeken. Overheidsdiensten kunnen op basis van meer informatie betere beslissingen nemen en met minder middelen toe. Handig, efficiënt en effectief voor de overheid én de burger.

In theorie dan. Want los van het gebrek aan overzicht, overkoepelende visie, transparantie en mogelijkheden voor burgers om grip te krijgen op hun privégegevens, benadrukken de WRR-onderzoekers nog een eigenschap van de iOverheid. Bij het verzamelen en koppelen van informatie worden fouten gemaakt. Fouten mét consequenties.

Die fouten, waarschuwden de auteurs, zijn geen uitzonderingen. 'Over de hele linie moet de assumptie dat informatie juist is vervangen worden door het besef dat de informatie op onderdelen hoogstwaarschijnlijk niet accuraat, verouderd en soms zelfs misbruikt en gemanipuleerd zal zijn.' En de burger? Die raakt verstrikt

in die informatiestromen. De dood van Alexander Dolmatov is een tragische uitzondering, de fouten die eraan ten grondslag lagen, zijn systemisch.

Je zou het ook kafkaësk kunnen noemen. In zijn meesterwerk *Het proces* beschrijft Franz Kafka op geniale wijze de uiterste consequentie van een ondoorgrondelijke overheid: een bureaucratische machine die machteloze burgers die erin terechtkomen kan vermalen.

In *Het proces* wordt hoofdpersoon Josef K. op een morgen van zijn bed gelicht. Medewerkers van De Rechtbank delen hem mee dat hij is aangeklaagd. Waarvoor of door wie vertellen zij er niet bij. Vanaf dat moment poogt K. zijn onschuld te bewijzen.

Hoe meer K. verdwaalt in de krochten en procedures van De Rechtbank – een analogie voor de overheid –, hoe frustrerender, absurder en hopelozer zijn zoektocht wordt. Overal binnen het systeem van De Rechtbank dwarrelt er informatie over K. rond, maar op elke plek ligt er weer een ander dossier. In plaats van stapje voor stapje de waarheid te ontrafelen, wordt De Rechtbank juist steeds ondoorgrondelijker en onbegrijpelijker. K. wordt paranoïde en beseft dat er geen antwoorden op zijn vragen zullen komen.

Als we het over privacy hebben, grijpen we vaak terug op een andere metafoor, die van Big Brother uit George Orwells boek *1984*. We kennen allemaal het beeld van het alziende oog van het totalitaire regime dat alles en iedereen monitort en controleert. In discussies over privacy en surveillance is de term 'orwelliaans' dan ook nooit ver weg. Toch ziet de Amerikaanse privacyjurist Daniel Solove in *Het proces* van Kafka een betere metafoor voor de dataslurpende en datadelende overheid van tegenwoordig.[40]

Het probleem, schrijft Solove, is niet zozeer dat al die informatie over ons verzameld wordt, het probleem is dat wij geen enkel zicht noch controle hebben op de manier waarop onze data worden gebruikt. In de woorden van Solove: 'Het probleem [...] is de macht die deze bureaucratieën over ons hebben.'

Nu zou je kunnen tegenwerpen: reuze interessant, maar Daniel Solove is een studeerkamergeleerde en Franz Kafka is een vroegtwintigste-eeuwse romancier. Wat heb ik daar als eenentwintigste-eeuwse wereldburger mee te maken? Het simpele antwoord: de bureaucratische hel waar Josef K. in terechtkomt bestaat. Vraag maar aan de nabestaanden van Alexander Dolmatov.

Meer slachtoffers van de bureaucratie

Een ander schrijnend slachtoffer van de datakluwen van de overheid is Ron Kowsoleea.[41] Deze Nederlandse zakenman stond meer dan vijftien jaar verkeerd geregistreerd in de databanken van verschillende Nederlandse overheidsdiensten. Kowsoleea kwam in de problemen doordat een drugsverslaafde oud-klasgenoot onder zijn naam misdrijven beging. Iedere keer dat de junk werd opgepakt, gaf hij de naam van Kowsoleea door.

Regelmatig werd Kowsoleea daardoor onterecht gearresteerd. Een keer werd hij door de Koninklijke Marechaussee uit een vliegtuig gehaald toen dat klaarstond om op te stijgen. Een andere keer kreeg hij gewapende agenten van de Fiscale inlichtingen- en opsporingsdienst (FIOD) over de vloer omdat ze dachten dat Kowsoleea de drugscrimineel was die ze zochten.

De verwoede pogingen van Kowsoleea om zijn naam te zuiveren, lezen als de nachtmerrie van Josef K. in *Het proces*. Het politiekorps in Amsterdam, waar Kowsoleea's oud-klasgenoot de meeste misdrijven pleegde, herstelde de foutieve informatie. Maar de Amsterdamse database was weer gekoppeld aan die van andere korpsen en eens in de 24 uur werd er informatie gesynchroniseerd, waardoor de fout weer de Amsterdamse database binnensloop. En terwijl het korps in Amsterdam wist dat Kowsoleea hier het slachtoffer was, had de FIOD weer eigen data waar ook de Marechaussee gebruik van maakte.

Zo bleef foutieve informatie aan Kowsoleea kleven, terwijl zijn leefwereld kleiner en kleiner werd. Op het laatst kwam hij niet meer buiten uit angst gearresteerd te worden.

Kowsoleea's voorbeeld is extreem, maar niet uniek. *De Monitor*, het onderzoeksjournalistieke programma van KRO-NCRV, hield lange tijd een dossier bij over mensen die verdwalen in de 'digitale doolhof' van de overheid.[42] Een kleine greep uit de vele voorbeelden: een vrouw ging in een verzorgingstehuis wonen en een andere bewoner werd door de fiscus als haar toeslagenpartner beschouwd. Niet alleen kon deze vrouw zijn persoonlijke gegevens via de site van de Belastingdienst zien, ook werden hun inkomens bij elkaar opgeteld, wat weer gevolgen had voor de hoogte van haar toeslag. Deze fout kwam bij meer mensen voor die *De Monitor* had opgespoord: doordat de Belastingdienst volslagen onbekenden als hun partner zag, liepen zij honderden euro's mis. En misschien nog wel het vervelendste: het kostte hun grote moeite de fouten ongedaan te maken, áls dit hun al lukte.

Wat leert dit nu? Dat onschuldige burgers domweg verstrikt kunnen raken in de datakluwen van de overheid. Een overheid die niet als een Big Brother neerkijkt op haar burgers en die haar toorn op hen laat neerdalen als iets haar niet bevalt. Nee, dit is een overheid die, vaak met de beste bedoelingen, voor zo ongeveer ieder probleempje een database optuigt en later koppelt aan een andere. Dit is een overheid die de regie over de datastromen van haar burgers kwijt is geraakt.

Terug naar de bijeenkomst op de burelen van *De Correspondent*. Het stoeien met overheidsdata gaat tot laat door op die mooie meidag in 2015. Het lukt de aanwezige hackers, datajournalisten en nerds de data enigszins te structureren. Heel veel data zijn opgeschoond en staan klaar om met andere data gecombineerd te worden.

Toch verliezen we de moed. Te veel informatie mist. We zijn bang nooit een volledig beeld te kunnen krijgen, laat staan een

zinvolle analyse te maken of een programma te bouwen waar mensen iets aan hebben als ze hun dataspoor willen volgen.

Om echt betrouwbare uitspraken te doen over de iOverheid moet er gewoon nog te veel gebeuren, met meer middelen en mankracht dan wij tot onze beschikking hebben. En hoewel dat als een nederlaag voelt, bevestigt het ook wat de WRR al beschreef: dat iedereen verstrikt raakt in de datakluwen van de overheid. Ook wij.

De rol van Google en Facebook

Gelijktijdig met ons onderzoek naar de informatiestromen van de Nederlandse overheid, verdiepen wij ons in commerciële surveillance. In het eerste deel van onze zoektocht ontdekten we dat het gedrag en de persoonlijke gegevens van iedere internetgebruiker prooi zijn voor een bonte verzameling partijen. Wij vonden trackers van bedrijven waar wij nog nooit van hadden gehoord. Nu willen wij weten: wie zijn deze datagraaiers? Waar gaan onze gegevens heen? Maar eerst kijken we naar verreweg de twee grootste digitale spionnen die wij maar al te goed kennen: Google en Facebook.

De reden dat Google en Facebook op de persoonlijke data van iedere internetgebruiker jagen is simpel: hoe beter zij ons kennen, hoe effectiever zij ons advertenties kunnen voorschotelen.

Laten we beginnen met Google.

Google werd in 1998 opgericht door de Amerikanen Larry Page en Sergey Brin. De twee vonden een antwoord op de wezenlijke vraag: hoe breng je orde aan in de chaos van al die miljoenen webpagina's die het internet toen vormden?

De oplossing van Brin en Page was even elegant als radicaal. Hun zoekmachine Google berekende de relevantie van sites en webpagina's. In 2016 klinkt dat vanzelfsprekend; halverwege de jaren negentig was dat revolutionair. De zoekmachines uit die tijd

bepaalden de volgorde van zoekresultaten door te tellen hoe vaak een zoekterm op een site voorkwam. Google berekent de relevantie van een site onder andere aan van het aantal links ernaartoe. Hoe meer links, hoe relevanter.

Hun tweede uitvinding – eigenlijk een synthese van bestaande ideeën plus wat inventief jatwerk – was zo mogelijk nog revolutionairder. Waar ieder internetbedrijf begin deze eeuw wanhopig op zoek was naar een verdienmodel, introduceerde Google er in 2002 een waarmee het bedrijf in relatief korte tijd een van de grootste en machtigste bedrijven ter wereld zou worden: AdWords, kleine tekstadvertenties die bij de resultaten van een zoekopdracht verschijnen. Je kent het wel: je zoekt naar een auto in de zoekmachine en krijgt een advertentie van Toyota te zien. Pas als je erop klikt, moeten adverteerders Google betalen. Adverteerder blij, want die kon plotseling zien of een advertentie werkte, en Google blij, want AdWords was de melkkoe die de expansiedrift van het bedrijf uit Silicon Valley kon financieren.

Ongeveer een jaar later kwam Google met nog een advertentiemodel, AdSense, dat van Google dé advertentiemakelaar van het internet heeft gemaakt. Met AdSense treedt Google op als bemiddelaar tussen websites en adverteerders. De websites krijgen advertenties die zo relevant mogelijk zijn voor hun bezoekers, Google krijgt een deel van de opbrengsten.

Dit ging nog over simpele rechttoe rechtaan advertenties. Dat veranderde in 2007, toen Google voor 3,1 miljard dollar DoubleClick kocht. Dit online advertentiebedrijf had een totaal andere aanpak dan Google: het beloofde adverteerders dat het 'meer dan honderd eigenschappen' van websitebezoekers bijhield in een database. Zoals: welke advertenties zij bekeken, hoelang zij ernaar keken, hoe zij over een pagina scrolden, op welke links zij klikten, welke producten zij interessant vonden, welke producten zij ook echt kochten en hoeveel zij daarbij uitgaven. Met de aankoop van DoubleClick werd Google een bedrijf dat ook het gedrag van miljoenen internetgebruikers gedetailleerd bij ging houden en werd

het, in de woorden van technologiejournalist Steven Levy, 'de krachtigste trackingtool van het web,' die 'een gebruiker kan volgen tot aan elke uithoek van het internet.'

In de jaren die volgden, kwamen er steeds meer gratis diensten onder de Googleparaplu te hangen. Gmail. Google Calendar. YouTube (dat Google in 2006 kocht). Google Drive. Ook bouwde Google een besturingssysteem voor smartphones, Android, en gaf dat gratis weg om zo veel mogelijk gebruikers te krijgen (met succes: ruim 70 procent van de smartphones draait op Android). Het bedrijf lanceerde ook Google Play, waar je apps, boeken, muziek, tijdschriften en films voor op je smartphone, tablet of laptop kunt kopen.

En daar houdt het nog niet op. In Amerika legt het bedrijf glasvezelkabels aan in gebieden met slechte internetconnectie. Google Hangouts moet de concurrentie met Skype aangaan. Bedrijven kunnen gratis hun webverkeer doorgronden met Google Analytics. Google helpt mee een goedkope laptop te maken en is nu bezig het internet in arme landen aan te leggen en te verbeteren. Er is een zelfrijdende auto ontwikkeld en een smartbril. Google is in virtual reality gegaan en koopt robotbedrijven op. En sinds 2014 komt Google ook je huis binnen door Nest op te kopen, een bedrijf dat een smartthermostaat maakt, en met Google Home, een virtuele assistent.

Dat Googles tentakels ver reiken, zagen we ook in ons onderzoek naar trackers. Op 73 van de 89 onderzochte sites kwamen wij het bedrijf tegen. In ons smartphoneonderzoek bleek het beeld niet veel anders. De 85 onderzochte apps maakten meer dan 4.000 keer contact met een Googleserver.

Recent onderzoek onder leiding van vooraanstaand surveillance-expert Chris Jay Hoofnagle laat zien dat de greep van het bedrijf op het internet in de Verenigde Staten vrijwel alomvattend is. Op de 1.000 populairste sites in de Verenigde Staten vonden de onderzoekers op 923 sites cookies van Google Analytics, DoubleClick en YouTube.[43]

Google kent onze gedachten, onze ideeën, onze sociale netwerken, onze dagschema's en onze mailconversaties. Het weet waaraan we werken, wie wij ontmoeten en waar we dat allemaal doen. Zo verwoordt CEO Eric Schmidt het zelf: 'We weten wie je bent. We weten waar je bent geweest. We kunnen min of meer weten waar je aan denkt.'

Ter ere van Googles zestienjarige verjaardag analyseren wij in september 2014 enkele beloften die het bedrijf gedurende zijn bestaan in het openbaar had gedaan. En we ontdekten een opvallend patroon. Een kleine greep:

- Oprichters Sergey Brin en Larry Page beloofden bij oprichting (1998) geen advertenties bij zoekresultaten te tonen. Die belofte werd in 2002 verbroken.
- Brin en Page beloofden geen gebruikersprofielen te gebruiken bij het leveren van advertenties. Die belofte werd in 2007 verbroken.
- Google zou nooit de data van de verschillende diensten – YouTube, Gmail, Calendar – samenvoegen. Die belofte werd op 24 januari 2012 verbroken, waardoor onderwerpen van onze intiemste mailconversaties nu verbonden kunnen worden met waar we ons bevinden.
- En Google beloofde niet zomaar informatie die het bedrijf verzamelt met DoubleClick te koppelen aan andere gegevens. Gebruikers moesten daar expliciet toestemming voor geven. Tot ook die belofte in juni 2016 werd verbroken. Voortaan moeten gebruikers het expliciet aangeven als zij *niet* willen dat al die informatiestromen gekoppeld worden.

Daarmee wordt ook het doel duidelijk dat Google met al die prachtige gratis diensten nastreeft: mensen naar zijn platform halen, verleiden om zo veel mogelijk data te delen, zodat Google zo effectief mogelijk advertenties kan verkopen.

Google, dat sinds kort onder de holding Alphabet Inc. valt, behaalt zo een jaaromzet van ongeveer 70 miljard euro en heeft meer dan 60.000 werknemers. Al die mensen, al die diensten worden vrijwel geheel betaald met inkomsten uit advertenties.

De enige partij wier tentakels over het internet en onze data vergelijkbaar zijn met Google, is Facebook. Gebruikers betalen voor het 'gratis' Facebook met hun persoonlijke gegevens. Iedere nieuwe gebruiker is een nieuw advertentiedoelwit. Facebook weet ontzettend veel over zijn gebruikers. Ga maar na welke informatie je zelf als gebruiker allemaal aan het bedrijf geeft. Dat staat nog los van de lessen die het bedrijf over jou trekt aan de hand van de analyse van jouw gedrag op het platform en het gedrag van jouw vrienden. En hoe beter Facebook zijn gebruikers doorgrondt, hoe gedetailleerder de informatie over de gebruikers die Facebook aan adverteerders kan verkopen.

Facebook is jonger dan Google. Mark Zuckerberg en een paar vrienden richtten de site op in 2004, toen ze aan Harvard studeerden. Vanaf 2010 begon het bedrijf keihard te groeien. De belangrijkste motor achter die groei was niet de bouw van snellere servers of een goede reclamecampagne, maar de toevoeging van een simpele knop: de *like button.*

Vóór de introductie van de vind-ik-leuk-knop was Facebook een relatief gesloten platform. Je logde in en communiceerde en deelde met vrienden op het platform. Met de introductie van de vind-ik-leuk-knop konden ook artikelen, filmpjes en websites buiten je eigen vriendenkring en buiten Facebook geliket worden.

Websites als nu.nl of ad.nl plaatsen tegenwoordig gretig de vind-ik-leuk-knop op hun site om meer bezoekers en dus meer advertentie-inkomsten te genereren. Ook websites die niet van advertenties afhankelijk zijn, kunnen niet meer om Facebook heen. Voor iedere website die wil groeien, is Facebook onmisbaar.

Neem *De Correspondent.* In juni 2016 heeft ons platform rond de 50.000 betalende leden en bijna 150.000 *likes* op Facebook. En dat merken we. De helft van onze bezoekers komt via Facebook.

Nu is *De Correspondent* niet afhankelijk van advertentie-inkomsten, maar er is wel een correlatie tussen hoe vaak onze stukken op Facebook worden gedeeld en hoeveel mensen betalend lid worden.[44]

Met de vind-ik-leuk-knop creëerde Facebook veel meer activiteit op zijn platform. Ook kreeg het bedrijf inzicht in wat mensen buiten Facebook om doen. Het sociale netwerk kan met de knop namelijk niet alleen het gedrag van gebruikers volgen, ook niet-gebruikers zijn nu in het vizier.

Dit ontdekte de Tilburgse onderzoeker Arnold Roosendaal in 2011. Elke bezoeker van een site met een vind-ik-leuk-knop krijgt van Facebook een cookie. Daarmee volgt Facebook het internetgedrag van zo goed als iedereen, want de knop is op meer dan tien miljoen sites geïnstalleerd. Ook als je Facebook opzegt, blijft het bedrijf je volgen.

En de analyse die wij maakten van het structureel verbreken van beloften door Google over het gebruik van gegevens, hadden wij evenzogoed van Facebook kunnen maken. Een uitgebreide Harvardstudie liet in 2016 zien dat de privacyvoorwaarden van Facebook in de loop der jaren consequent minder transparant zijn geworden over wat er nu precies verzameld wordt en wat er met die persoonlijke informatie gebeurt.[45] In 2009 paste Facebook bijvoorbeeld grondig de privacyinstellingen aan. Zuckerberg vertelde dat de instellingen werden vereenvoudigd om ze voor de gebruikers overzichtelijker te maken. Later bleek wat Zuckerberg met 'overzichtelijker' bedoelde: met de nieuwe standaardinstellingen werden veel meer data over die gebruiker gebruikt dan voorheen. Zuckerberg bood later zijn excuses hiervoor aan. Dat moest hij ook doen in 2011, toen Facebook een schikking trof met de Amerikaanse toezichthouder FTC. Facebook had zijn klanten misleid, en niet zo'n klein beetje ook. Zo beloofde Facebook dat het data van gebruikers niet met adverteerders zou delen. Dat deed het wel. Verzekerde het zijn gebruikers dat als zij hun accounts deactiveerden of verwijderden, hun foto's en video's niet meer kon-

den worden bekeken. Dat bleek een leugen. En stelde het bedrijf gebruikers gerust door te beloven dat bepaalde informatie privé zou blijven. Ook dit bleek niet waar te zijn.

Voor de duidelijkheid: ook wij gebruiken Google en Facebook. De bedrijven maken prachtige producten. Zonder beide bedrijven zou ons leven én werk als journalist een stuk moeilijker zijn. Beide bedrijven doen ook waanzinnig interessant onderzoek op het gebied van data-analyse en kunstmatige intelligentie. En hun duizelingwekkende groei dwingt respect af.

Maar laten we onszelf niet voor de gek houden. Facebook en Google zijn geen publieke diensten. Het zijn immens succesvolle advertentiebedrijven. Om een idee te krijgen: volgens schattingen ging in het eerste kwartaal van 2016 maar liefst 85 cent van iedere dollar die online aan advertenties is gespendeerd naar Facebook of Google.[46] En wij? Wij zijn geen klanten van Facebook en Google, wij zijn hun producten. Zelfs als wij hun diensten niet gebruiken.

Wat datamakelaars over ons weten

Tijdens ons onderzoek naar trackers op laptops en smartphones komen we nog een ander type bedrijf tegen dat grof geld verdien aan onze data. Dit type bedrijf verkoopt zoals Google of Faceboo geen advertenties, maar handelt uitsluitend in de verzameld data.

Van veel van de bedrijven die wij aantreffen, hebben we no nooit gehoord: Omniture, Rubicon, Improve Digital, Metrigo Burst Media, Sociomantic, Yieldlab, Smart Adserver, OpenX. Som mige blijken omzetten van miljarden dollars te draaien en data i huis te hebben van honderden miljoenen internetters. Hoe ka dat?

Datamakelaars verkopen gedetailleerde on- en offline informa tie over internetters door aan adverteerders en marketeers. Z

hebben zowel informatie over ons uit de fysieke wereld als over ons digitale doen en laten. Wil je weten wie er in een bepaald gebied zwanger is? Wie er gescheiden is en wie graag dure televisies koopt? Of wil je een lijst van notoire wanbetalers of mensen die alleen op goedkope aanbiedingen ingaan? Een datamakelaar kan het je vertellen. Tegen betaling, uiteraard.

Neem het bedrijf Metrigo, dat op zijn website schrijft: 'In plaats van bestaande klanten te benaderen, gebruiken we verfijnde en complexe data-analyse om statistische dubbelgangers te vinden en ze te benaderen met gepersonaliseerde boodschappen.'

De website van een ander bedrijf, Sociomantic, toont een foto van een vrouw bij een stapel schoenendozen. De titel: *fashion addict*. Met daaronder enkele wetenswaardigheden over de vrouw. Productcategorie waar ze het meest naar gesurft heeft: schoenen. Schoenmaat: 38. Gemiddeld totaalbedrag van de producten in haar winkelwagentje: 421,55 euro.

In totaal komen wij 51 datamakelaars tegen in ons onderzoek naar trackers. Op hyves.nl treffen wij een cookie aan van de bekendste datamakelaar ter wereld, het Amerikaanse bedrijf Acxiom (werkterrein naar eigen zeggen: *audience solutions, data and decision science*). Deze handelaar behaalde in 2015 een omzet van 1,15 miljard dollar en beweert in het bezit te zijn van gedetailleerde informatie over meer dan 700 miljoen consumenten wereldwijd die 'continu wordt geüpdatet.'

Op nu.nl, hyves.nl en voetbalzone.nl vinden we cookies van een ander Amerikaans bedrijf, Datalogix, gespecialiseerd in de analyse van aankoopgedrag van consumenten. Op de site van het bedrijf is bijvoorbeeld informatie te koop over mensen die geregeld dieetpillen aanschaffen of in de winter vaak verkouden zijn en daar medicijnen voor bestellen. Ook kunnen adverteerders bij Datalogix terecht als zij geïnteresseerd zijn in vrouwen die voldoen aan het profiel 'huismoeder' of 'vrouwen die vaak naar talkshows kijken.'

Terwijl wij dergelijke bedrijven onder de loep nemen, komt er een stevig rapport uit van de Amerikaanse toezichthouder Federal Trade Commission (FTC). In die datahandelsector, concludeert de FTC, heerst een 'fundamenteel gebrek aan transparantie.'[47] Verreweg de meeste consumenten kennen de sector en de bedrijven niet, laat staan dat zij weten dat er 'immense hoeveelheden data' over hen worden verzameld, uitgewisseld en verkocht. Een van de bedrijven die de FTC onder de loep neemt bezit data over 1,4 miljard consumententransacties en 700 miljard '*data elements*' en voegt iedere maand meer dan 3 miljard nieuwe gegevens aan zijn database toe.

Het is eigenlijk ondenkbaar, aldus de FTC, dat er Amerikanen zijn die niet in de databanken van de datahandelaren zijn terug te vinden. Databanken die door sommige handelaren voor altijd worden bewaard. 'De mate waarin consumenten worden geprofileerd, betekent dat de datahandelaren net zoveel van ons weten, zo niet meer, als onze familie en vrienden, inclusief onze online en offline aankopen, onze politieke en religieuze overtuigingen, ons inkomen, onze sociaal-economische status en nog veel meer.'

Datahandel in Nederland

Hoe zit dit in Nederland? Collega Maaike Goslinga gaat op ons verzoek met die vraag op pad. Maandenlang zal zij zich verdiepen in de Nederlandse datamarkt, in de spelers, hun capaciteiten, de regels en het spel.

Ze ontdekt dat er in Nederland minstens 180 verschillende datahandelaren actief zijn, die in de persoonlijke informatie van alle Nederlanders handelen. Van de meeste bedrijven hebben we nog nooit gehoord: Experian, Graydon en Sandd kennen we van ons onderzoek naar de trackers, maar N.A.W.plus, WIJ Special Media, Elite-Miljonairs, 40range en Cendris zijn voor ons totaal onbekend. Terwijl zij ons heel goed zeggen te kennen.

N.A.W.plus blijkt een interessante makelaar. Dit bedrijf bezit uitvoerige lijsten van predikanten, pastoors en 'actieve christenen,' die het koopt van een uitgeverij van boeken en folders 'voor dagelijkse bezinning.' N.A.W.plus verkoopt ook de namen en adresgegevens van de bezoekers van een christelijk vakantiepark op de Veluwe. Het heeft de e-mailadressen van bezoekers van jongeren-community Refoweb én datingwebsite Christianmatch.

Databedrijf WIJ Special Media claimt 'nagenoeg alle' adressen van zwangere vrouwen in Nederland te hebben. Het bedrijf biedt gratis zwangerschapspakketten aan in ruil voor persoonlijke informatie als adresgegevens, geboortedatum, de uitgerekende datum, de naam en het geslacht van het kind.

Weer andere datahandelaren verhandelen contactgegevens van Nederlandse miljonairs, welgestelden en bekende Nederlanders. Zo betaal je bij Elite-Miljonairs onder het mom van hoe rijker, hoe duurder voor bekende Nederlanders 70 eurocent per adres en voor multimiljonairs 1,25 euro.

Handelaar 40range beweert gegevens van 'alle Nederlandse consumenten' te bezitten en biedt een zogenoemde 'lifestylescan van uw klantenbestand' aan. Het bedrijf kijkt dan naar de data van de klant en vergelijkt die met zijn eigen gegevens. Hiermee krijgen bedrijven een 'gedetailleerd inzicht in de karakteristieken van hun doelgroep aan de hand van een groot aantal kenmerken op het gebied van socio-demografie, koopgedrag, media en lifestyle.'

Het bedrijf Cendris 'helpt klanten communiceren op een manier die leidt tot meer resultaat.' Cendris kijkt bijvoorbeeld hoe uit bestaande klantgegevens een 'hogere conversie en meer loyaliteit' gehaald kunnen worden. Dit bedrijf is onderdeel van PostNL en levert producten en diensten op basis van de enorme hoeveelheid gegevens die PostNL over ons heeft.

Wat weten die bedrijven nu precies over ons? Maaike Goslinga besluit hiervoor, net als Douwe Schmidt eerder deed, gebruik te maken van haar wettelijke recht op inzage en stuurt 25 inzageverzoeken naar evenzoveel datahandelaren. Ze stelt de bedrijven drie simpele vragen: Heeft u persoonlijke gegevens van mij in huis? Zo ja, welke? En: wat doet u ermee?

Na twee maanden reageren vier van de 25 bedrijven – ondanks de wettelijke verplichting – helemaal niet, vier andere bedrijven vragen aanvullende informatie. Twee bedrijven antwoorden dat zijzelf geen databases in beheer hebben, maar klantbestanden van andere handelaren analyseren. Ja, zeggen ze, het is mogelijk dat Goslinga daarin staat, maar het is onmogelijk om daarachter te komen. Twaalf bedrijven zeggen helemaal niks van haar te weten. Drie datahandelaren schrijven wél gegevens over Goslinga te hebben.

Experian, een van de grootste datahandelaren ter wereld, schrijft dat bekend is waar ze woont, dat ze een vrouw is en dat ze een vaste telefoonaansluiting heeft. Sandd weet van alles over haar huis en woonomgeving. Graydon stuurt een kopie van haar bedrijfsgegevens mee, inclusief het aantal werknemers (één, zijzelf) en een zogenoemde kredietscore; een getal dat aangeeft hoe kredietwaardig Goslinga is.

Op het eerste oog zijn de drie reacties nogal summier. Toch leggen zij al een aantal interessante zaken bloot. Goslinga heeft namelijk nog nooit contact met deze partijen gehad. Dit betekent dat datahandelaren Experian, Sandd en Graydon die informatie van andere bronnen hebben verkregen. Het blijft vaag wie of wat die bronnen precies zijn. Zowel Sandd als Graydon schrijven dat ze 'openbaar' zijn, zonder dat te specificeren. Een medewerkster van Experian zegt dat het bedrijf toegang heeft tot 'een schat aan informatie van bronnen met registratiedata – zoals uitgebreide en gedetailleerde vastgoedgegevens en diverse personenbestanden.' Gevraagd naar welke bronnen dat precies zijn, is het antwoord 'bedrijfsgeheim.'

We kunnen zelf wel bedenken over welke openbare bronnen he[t] gaat: het Kadaster, het Handelsregister van de Kamer van Koop[handel]

handel, het Centraal Bureau voor de Statistiek. Veel van de informatie die datahandelaren daaruit halen, gaat niet zozeer over individuen, maar over wijken, straten en buurten. Vervolgens worden individuen die daar wonen ingedeeld in de categorie die bij die wijk, straat of buurt hoort.

Zo hanteert Experian een groepsprofiel met de naam 'Minder Geslaagden.' Dit zijn arme mensen die, volgens hun beschrijving, 'veel thuis zitten' en daardoor 'kunnen nadenken over hoe het had kunnen zijn.' Ze wonen in 'vervallen wijken' met een 'ratjetoe' aan huizen en mensen. In hun huis hangen 'gordijnen voor de ramen' en staan 'vetplanten' op de vensterbank. Het is een beschrijving die Experian zelf heeft verzonnen. In geen enkele openbare bron staat of iemand een vetplant voor het raam heeft staan.

Als je dus woont in een straat die te boek staat als een straat van Minder Geslaagden, dan kan het zomaar zo zijn dat Experian jou ook als een Minder Geslaagde beschouwt. Ook als je niet aan dat profiel voldoet en je, bijvoorbeeld, luxaflex voor de ramen hebt hangen, rode rozen op de vensterbank hebt staan, minstens een uur per dag jogt terwijl je denkt aan hoe gelukkig je wel niet bent.

Informatie van datahandelaren hoeft dus niet te kloppen. Ze is vaak een gemiddelde van een buurt, postcode, wijk, of andere groep. Voor Goslinga betekent dit dat Experian niet alleen haar adres kent en weet dat zij een vrouw is, maar ook denkt dat zij een jaar of 45 is, dol op beleggen, in een Volvo rondrijdt en graag de *Linda* leest.

Alleen: is Goslinga ten tijde van haar onderzoek 25 jaar oud, net afgestudeerd, zonder vaste baan en tijdelijk inwonend bij haar vader. Experian deelt haar op basis daarvan in bij het groepsprofiel 'Gouden Rand.' Anders dan mensen met de profielen 'Vergrijsde Eenvoud' en 'Sociale Huurders' is ze, als je naar haar wijk kijkt, waarschijnlijk rijk en een harde werker.

Goslinga slaagt er uiteindelijk niet in om inzicht te krijgen in de totstandkoming van haar profiel. Dit weigeren deze bedrijven te vertellen onder het mom van 'bedrijfsgeheim' en 'concurrentiegevoelig.' 'Handelsinformatiebureaus,' concludeert Goslinga in een artikel op *De Correspondent*, 'hóéven volgens de wet bovendien geen inzage te geven in de modellen die zij gebruiken [...]. Dit is concurrentiegevoelige informatie.'

Of dit mag? Ja, een bedrijf mag persoonlijke informatie aan andere bedrijven verkopen. Mits de klant goed en helder wordt geïnformeerd welke data er met wie worden gedeeld. En die kleine lettertjes, zo ontdekt Goslinga, zijn meestal diep begraven in de algemene voorwaarden waar je ooit akkoord mee bent gegaan.

Haar zoektocht toont aan: ook al heb je niets met een bedrijf te maken, toch kun je in zijn database terechtkomen. Dus stel dat je je benadeeld voelt, er een fout is gemaakt of je gewoon gebruik wilt maken van jouw wettelijk inzagerecht: kom er maar eens achter waar jouw data rondzwerven.

En soms heb je je gegevens wél bewust aan een bedrijf of organisatie gegeven en duiken die onverwacht op een heel andere plek op. Als je een donatie doet aan een goed doel, kun je gebeld worden door marketeers omdat je telefoonnummer doorverkocht is. En als je iets bestelt in een webshop, kan die je data doorverkopen aan marketingbedrijven.

In mei 2016 tekent *Volkskrant*-journalist Margriet Oostveen dit verhaal op. 'Op haar elfde verjaardag opent de dochter van Anne de Rooij de post. Hieperdepiep. Er is een vrolijke envelop bij, versierd met smileys en de tekst 'Kleine meisjes worden groot...'. Dochter trekt er twee stuks maandverband uit. Een inlegkruisje. En een informatieboekje voor ouders, bedoeld voor een eerste gesprek over menstruatie. Met de groeten van Always, ofwel maandverbandfabrikant Procter & Gamble.'[48]

Anne de Rooij wil weten hoe haar dochter dit 'geschenk' kon ontvangen. Na wat rondbellen komt ze erachter dat de voetbalbond KNVB – haar dochter zat een tijdje op voetbal – informatie over haar dochter heeft doorverkocht aan databeheerbedrijf EDM. De directeur van EDM vertelt Oostveen dat zijn bedrijf gebruikmaakt

van een statistisch scoringsmodel dat de kans berekent dat op een bepaald adres een meisje woont dat voor het eerst ongesteld wordt. Blijkbaar zorgen die KNVB-data voor een heel betrouwbare score, zegt de directeur.

Een zwangerschap verbergen – kan dat wel?

Als zelfs elfjarige meisjes doelwit zijn van datahandelaren, kun je dan überhaupt nog uit hun vizier blijven? De Amerikaanse Janet Vertesi nam in 2013 de proef op de som. De technologiesocioloog wilde kijken of het mogelijk was haar zwangerschap voor online bedrijven, adverteerders en marketeers verborgen te houden.

Dat bleek een hele klus.

Zo moest ze op Facebook en Twitter over haar zwangerschap zwijgen. Ze belde al haar kennissen en vrienden op met het verzoek er niets over te zeggen. Dat ging niet goed. Enkele familieleden stuurden toch een privébericht op Facebook om haar te feliciteren in de veronderstelling dat privé echt privé betekent. Die familieleden werden door Vertesi subiet ontvriend. Het online zoeken naar flesjes, kleren en andere babyspullen deed ze met anonimiseringssoftware Tor. Met contant geld kocht ze Amazon-cadeaubonnen waarmee ze op internet spullen kon aanschaffen. Op die manier liet ze geen spoor achter naar haar bankrekening en dus niet naar haar identiteit. De babyspulletjes liet Vertesi bezorgen bij een postbus bij haar in de buurt. Dat ging goed. Totdat haar man op een dag in de winkel bij de aanschaf van een grote hoeveelheid cadeaubonnen te horen kreeg dat hij aangegeven kon worden voor witwassen.

Anonimiseringssoftware. Een postbus. Aangemerkt worden als witwasser. 'Mijn pogingen om aan het Big Data-sleepnet te ontsnappen maakten me niet alleen een onbeschoft familielid en een tactloze vriend, ik leek ook steeds meer op een kwaadwillende burger,' verzuchtte Vertesi in een artikel over haar ervaringen.[49]

De sleepnetten van de datamakelaars zijn kortom niet te ontwijken. Wie een normaal leven wil leiden, zal dit soort commerciële surveillance op de koop toe moeten nemen en moeten accepteren het middelpunt van een wereldwijd web van informatiestromen te zijn.

Hoe private en publieke netwerken versmelten

Toen wij aan ons onderzoek naar datastromen begonnen, zagen wij surveillance door bedrijven en overheden als twee gescheiden werelden. Gaandeweg kwamen we erachter dat die werelden samenvallen. De Amerikaanse cryptograaf Bruce Schneier, die we eerder aanhaalden om duidelijk te maken waarom we onze gegevens niet beter beveiligen, noemt het zelfs een publiek-private surveillancesamenwerking: een systeem waarbinnen bedrijven en overheden wereldwijd informatie uitwisselen.

Die samenwerking is inderdaad op veel terreinen aanwijsbaar. De Nederlandse politie maakt gebruik van de diensten van Coosto, een Eindhovens bedrijf dat alle socialemedia-uitingen in Nederland bewaart en doorzoekbaar maakt. Bij grote evenementen kan de politie potentiële raddraaiers tijdig vinden. TomTom en Google en de gemeente Amsterdam werken samen om aan de hand van locatiedata verkeersstromen in de stad in kaart te brengen. De gemeente Amsterdam krijgt ook gegevens van het sociale netwerk LinkedIn, zodat ze gericht arbeidsmarktbeleid kan voeren. Andersom kopen veel bedrijven data uit het Handelsregister van de Kamer van Koophandel en het Kadaster om consumenten en bedrijven te kunnen beoordelen, zoals Maaike Goslinga ondervond. Google maakt weer gebruik van file-informatie – die gegenereerd wordt door sensoren van Rijkswaterstaat langs de snelwegen – om de gebruikers van Google Maps een accurate inschatting van hun reistijd te geven.

En de belangrijkste les van de onthullingen van Edward Snowden is dat inlichtingendiensten ons niet rechtstreeks bespioneren, nee, zij bespioneren Google, Microsoft, Facebook, Yahoo! en andere advertentiebedrijven die ons bespioneren. Inlichtingen- en veiligheidsdiensten hoeven helemaal geen dure infrastructuur op te zetten om massasurveillance mogelijk te maken: ze halen de data simpelweg bij commerciële technologiebedrijven.

In Nederland is de versmelting van private en publieke surveillance ook in de wet vastgelegd. In 2005 werd de Wet bevoegdheden vorderen gegevens van kracht. Met deze wet kunnen politie en justitie gegevens als namen, telefoonnummers, e-mails, belgeschiedenissen, locatiegegevens en meer opvragen bij bedrijven en instellingen – die verplicht zijn om mee te werken.

Op het moment dat wij dit schrijven, ligt een wetsvoorstel in de Tweede Kamer dat de bevoegdheden van inlichtingendiensten aanzienlijk uitbreidt. Als het aan de regering ligt, mogen de AIVD en de MIVD straks complete databases opvragen bij bedrijven en instellingen om die te doorzoeken op bijvoorbeeld aanwijzingen voor terroristisch gedrag. De bedrijven en instellingen zijn volgens het laatste wetsvoorstel overigens niet verplicht hieraan mee te werken. Ook mogen AIVD en MIVD, aldus het voorstel, ongericht internetkabels aftappen en bijvoorbeeld naar verdachte woorden zoeken. Ook hier geldt: de diensten zetten niet zelf een surveillancesysteem op, ze haken in op bestaande, vaak commerciële, infrastructuur.

Data van Nederlandse burgers gaan niet alleen rond bij Nederlandse bedrijven en overheden, ook Amerikaanse private en publieke instellingen kunnen daar – in theorie – bij. De Amerikaanse opsporings- en inlichtingendiensten hebben een flink juridisch arsenaal tot hun beschikking om data te vergaren. Ook van Nederlanders. Bekend is de PATRIOT Act, die kort na de aanslagen op de Twin Towers werd aangenomen. De FBI mag sindsdien wereldwijd bij bedrijven en organisaties informatie opvragen, zoals documenten en data over telefoon- en e-mailverkeer. Bedrijven die dit weigeren, overtreden de Amerikaanse wet.

Een interessante vraag is: wat is er bij de Nederlandse overheid bekend over het opvragen van Nederlandse data door Amerikaanse inlichtingendiensten? In de Nederlandse Grondwet staat dat de regering verplicht is haar burgers te beschermen. Wat heeft de regering de afgelopen jaren gedaan om potentieel bedreigende wetgeving in de VS te bestrijden en agressieve interpretaties ervan te voorkomen?

In 2014 vragen we bij zes ministeries met behulp van de Wet openbaarheid van bestuur documenten op over hoe ze met de PATRIOT Act omgaan. We ontvangen een verslag van een bijeenkomst uit 2013 over de PATRIOT Act op het ministerie van Financiën. Tijdens die bijeenkomst vertelt specialist Lokke Moerel van De Brauw Advocaten over de enorme reikwijdte van de PATRIOT Act. Ze legt uit dat de wet van toepassing is als er een *band bestaat* met Amerika. Daar is al sprake van als een Nederlands bedrijf of een Nederlandse organisatie een 'continue en systematische' activiteit op Amerikaanse bodem heeft. Het is dus geen vereiste dat het hoofdkantoor in Amerika staat. Als een Amerikaanse vestiging toegang heeft tot gegevens buiten Amerika (bijvoorbeeld van het Europese hoofdkantoor), moeten die ook worden afgegeven. Ook medewerkers met de Amerikaanse nationaliteit die toegang hebben tot bijvoorbeeld een datacentrum in Nederland kunnen door de FBI of NSA tot afgifte worden verplicht.

Naast de PATRIOT Act is er de Foreign Intelligence Surveillance Act (FISA), waarmee Amerikaanse bedrijven gedwongen kunnen worden dataverkeer te onderscheppen, bijvoorbeeld door het plaatsen van taps in het glasvezelnetwerk.

In 2008 is daar nog de FISA Amendments Act bij gekomen. Op basis van deze wet kunnen opsporings- en veiligheidsdiensten gegevens over niet-Amerikanen opvragen bij cloud-providers als

het veelgebruikte Dropbox of Google Drive. Die providers krijgen een vergoeding voor hun medewerking.

Een van de bedrijven die van Amerikaanse inlichtingendiensten taps moeten plaatsen in hun netwerk is Level 3 Communications, dat een groot deel van het wereldomspannende netwerk van glasvezelkabels en routers beheert. Tussen één derde tot de helft van het wereldwijde internetverkeer loopt via de kabels van Level 3 Communications.

Het bedrijf heeft ook veel infrastructuur in Nederland en Europa. Allerlei partijen – privaat en publiek – maken gebruik van zijn netwerk. In het verleden was KPN klant bij Level 3 Communications – het bedrijf wil ons niet vertellen of dat nog steeds het geval is. Ook grote bedrijven met veel dataverkeer, zoals financiële instellingen, maken gebruik van Level 3-kabels. In Nederland heeft het bedrijf kabels lopen tussen de grote steden in de Randstad en vanuit Nederland kabels naar Brussel, Parijs, Straatsburg, Keulen, Hamburg en Frankfurt. Stuk voor stuk economisch en politiek belangrijke steden. Omdat Level 3 een Amerikaans bedrijf is en onder de PATRIOT Act en FISA valt, zijn de data die door de kabels van het bedrijf stromen opvraagbaar door Amerikaanse diensten.

Een ander bedrijf dat wereldwijd veel datacentra bezit, is het Amerikaanse Equinix. Dit bedrijf beheert ook data van onze Rijksoverheid, onder andere van Rijkswaterstaat, de Dienst Justitiële Inrichtingen en het Rijksinstituut voor Volksgezondheid en Milieu. De overheid wil haar data niet in het buitenland opslaan en heeft daarom een cloud bij Equinix in Amsterdam laten inrichten. Met een bevel op basis van de PATRIOT Act of de FISA kunnen de Amerikaanse inlichtingendiensten er toch bij komen: Equinix is immers een Amerikaans bedrijf.

Benadrukt moet hier worden dat we geen concrete aanwijzingen hebben dat de genoemde bedrijven daadwerkelijk Nederlandse data onderscheppen en overdragen aan Amerikaanse opsporings-

en veiligheidsdiensten. Daar is ook bijna niet achter te komen. Want, zo legt specialist Lokke Moerel uit als we haar later spreken: 'Medewerkers van een Amerikaanse vestiging die de onderschepping uitvoeren, krijgen *gagging orders*. Ze mogen met niemand over de verzoeken praten, soms niet eens met hun eigen directie.'

Ondanks deze geheimzinnigheid is Moerel stellig over wat de Amerikaanse diensten kunnen. 'Staat het hoofdkantoor van een bedrijf in de Verenigde Staten en bezit het in Nederland netwerken of andere infrastructuur, dan kunnen de Amerikaanse veiligheidsdiensten bij de data komen. Geen twijfel over mogelijk. Dit wordt ook niet ontkend.'

Dat de Amerikaanse diensten inzageverzoeken doen bij bedrijven, werd ook door president Barack Obama erkend. Enkele technologiebedrijven, waaronder Google, Facebook en Twitter, hebben bedongen dat ze een indicatie van het aantal verzoeken op basis van de FISA mogen publiceren. Sindsdien weten we dat de meeste grote internetbedrijven enkele tienduizenden informatieverzoeken per jaar krijgen.

Ondertussen blijkt uit de documenten die we op basis van de Wob ontvangen dat de Nederlandse overheid hier wel van op de hoogte is, maar bar weinig actie onderneemt.

Uit een verslag van Binnenlandse Zaken valt op te maken dat de overheid flink achterloopt op het bedrijfsleven in het beschermen van haar gegevens en infrastructuur. Zij refereren in documenten aan de bijeenkomst uit 2013 met advocaat Lokke Moerel. '[Moerel] deelt ons [de aanwezige ambtenaren] in haar verbazing over het grote verschil in de wijze waarop de (Nederlandse) overheid en de multinationals in haar klantenbestand omgaan met risico's die verband houden met internationale wetten zoals de PATRIOT Act,' zo vermeldt het verslag.

Volgens Moerel maken multinationals grote kosten om hun data uit handen van andere landen te houden. Ook maken ze duidelijke afspraken met ICT-leveranciers over wat, wanneer aan wie

mag worden verstrekt. De overheid maakt die afspraken met leveranciers niet of veel te laat.

Dus, wat kan de burger nu doen?

Onze zoektocht naar de datastromen bij de Nederlandse overheid, commerciële partijen en de samenwerking tussen die twee, levert een verontrustend beeld op. Beide verzamelen niet alleen gigantisch veel informatie over ons allemaal op vaak ondoorzichtige wijze, wij – burgers en consumenten – staan hier ook machteloos tegenover.

Ja, formeel heb je controle. Je kunt gebruikmaken van je inzagerecht. Google biedt je de mogelijkheid om je persoonlijke informatie in te zien en te wissen. Vrijwel alle datahandelaren die we zijn tegengekomen hebben uitvoerige algemene voorwaarden. Maar, zo blijkt uit ons onderzoek, veel is dat allemaal niet waard als je precies wilt weten wat er met jouw gegevens gebeurt.

Op een prachtige dag in mei 2016 spreken we af met de twee belangrijkste auteurs van het rapport *iOverheid*: Corien Prins en Dennis Broeders. Wij ontmoeten hen in Villa Augustus, een restaurant en hotel in een verbouwde watertoren in Dordrecht. Prins heeft de WRR verlaten en is hoogleraar en decaan aan de Universiteit van Tilburg. Broeders werkt nog bij de WRR en zal een paar dagen na ons gesprek een nieuw omvangrijk rapport publiceren: *Big Data in een vrije en veilige samenleving*.[50]

Vijf jaar na verschijning van *iOverheid* is de kluwen van informatiestromen alleen maar groter geworden. Kijken de onderzoekers dus ook anders naar die datahonger en de verknoping van al die publieke en private datastromen?

Broeders en Prins zijn allereerst trots op de impact die hun rapport heeft gehad. Ze merken dat bestuurders binnen de Rijksoverheid

nu echt beseffen dat ze deel uitmaken van een iOverheid en dat ze dus verantwoordelijk zijn voor de dataspaghetti. Prins vertelt bijvoorbeeld dat ze een keer na een lezing werd aangeschoten door een hoofdcommissaris van de politie. De hoofdcommissaris wilde, met *iOverheid* in gedachten, eens praten over waar de grenzen in zijn organisatie liggen en hoe hij die inzichten in de hoofden van iedereen binnen de politieorganisatie kon krijgen.

Veel politici daarentegen negeerden het rapport. Broeders: 'Dat techno-optimisme, waarbij voor ieder probleem een database moet worden opgericht en informatie moet worden uitgewisseld, is nog steeds *alive and kicking*.' En nog steeds heeft niemand het overzicht, laat staan dat er iemand sturing kan geven aan de immer uitdijende gegevensverzameling.

Dus ja, de twee staan nog steeds achter de inhoud van het rapport. Wel is er een aantal inzichten bij gekomen. De datahonger is niet te stoppen, zegt Prins. 'Ik ben er steeds meer van overtuigd dat je eigenlijk niet meer moet inzetten op de rechten van de burger.'

We kijken verbaasd op. Dit is nogal een uitspraak.

Ze legt uit dat een van de hoekstenen van het privacyrecht, dat burgers hun informatie bij derden kunnen inzien, niet bruikbaar is. Als je bedrijven en overheden om informatie vraagt, kom je al snel in slepende procedures terecht en krijg je vaak niet wat je wilt. Een inzicht dat Douwe Schmidt en Maaike Goslinga na hun datazoektocht kunnen beamen.

Een dergelijke vorm van controle legt ook veel te veel verantwoordelijkheid bij de burger, vindt Prins. Tegenmacht aan datahongerige bedrijven en overheden moet op een hoger niveau worden georganiseerd: bij een sterke toezichthouder en de rechterlijke macht. 'Natuurlijk moeten we het recht op inzage behouden, maar je kunt gewoon niet verlangen dat een burger dan vervolgens in zijn eentje zijn recht kan halen.'

Vijf jaar na publicatie van het rapport is er bovendien een cruciale technologische ontwikkeling bij gekomen die in *iOverheid*

nog geen noemenswaardige rol speelde: Big Data. Waar Big Data precies voor staat, daar zijn de meningen over verdeeld, maar in essentie gaat het over enorme hoeveelheden gegevens die worden geanalyseerd en waaruit lessen worden getrokken over het gedrag van grote groepen mensen. De afgelopen jaren heeft de Nederlandse overheid allerlei Big Data-toepassingen omarmd. Van inlichtingendiensten die er terroristen mee pogen op te sporen tot de Belastingdienst en het ministerie van Sociale Zaken die er fraudeurs mee proberen te detecteren. Broeders heeft net een rapport voor de WRR afgerond over Big Data. En ook Prins heeft haar aandacht de afgelopen jaren verlegd naar deze nieuwe ontwikkeling. Een Big Data-overheid, ontdekken wij tijdens het gesprek met de twee professoren, is een iOverheid *on steroids*, die de relatie tussen overheid en burger nog meer onder druk zet. Dennis Broeders: 'Er kan veel goeds uit Big Data-analyses komen, mits je rekening houdt met de beperkingen. Maar ga dat maar eens aan een politicus uitleggen. De meeste Big Data-systemen van de overheid zijn black boxes. Niemand bij de overheid begrijpt echt hoe ze werken. Daar komt nog bij dat private partijen die algoritmes bouwen. Ze zijn bedrijfsgeheim. Om het even dramatisch aan te zetten: een overheidssysteem dat uiteindelijk ingezet wordt op basis van de zwaardmacht van de overheid, heeft een kern, een algoritmisch hart, waar de overheid zelf ook niet in mag kijken.'

En de burger? Die heeft geen idee wat er in al die black boxes met zijn gegevens gebeurt en welke beslissingen er voor en over hem worden genomen. Broeders: 'De huidige wetgeving gaat vooral over het verzamelen en delen van informatie. Maar we zouden eens moeten gaan kijken naar hoe die informatie wordt gebruikt.'

'We doden mensen op basis van metadata.'[51]

– OUD-NSA-DIRECTEUR MICHAEL HAYDEN

'De briljantste geesten van mijn generatie denken na over hoe ze mensen het best op advertenties kunnen laten klikken.'[52]

– EX-FACEBOOKMEDEWERKER JEFFREY HAMMERBACHER

4

Surveillancekapitalisten en sturende overheden

Waarom de jacht op onze gedragsgegevens definitief is geopend

Ton Siedsma is nerveus. Hij heeft enkele weken geleden al beslo-ten dat hij het doet, maar stelt de uitvoering telkens uit. Als hij op een koude herfstavond om tien over acht op weg naar huis station Elst passeert, activeert hij toch de app. Het experiment begint.

Siedsma zal zijn normale leven blijven leiden. Hij zal iedere doordeweekse dag vanuit zijn huis in Nijmegen met de fiets en de trein naar zijn werk in Amsterdam gaan. Op zaterdag zal hij met de auto naar Den Bosch gaan om in de buurt van het Zuiderpark te overnachten. Vervolgens zal hij met het openbaar vervoer terug naar Nijmegen gaan. Om later op de dag nog wat te drinken in café St. Anneke in Nijmegen.

Niets geks dus. Behalve die app dan. Die staat vanaf nu continu aan. En registreert alle metadata die door Siedsma's telefoon gaan. Na een week zal Siedsma die data aan ons overhandigen. Alleen als anderen daardoor geschaad kunnen worden, mag hij die censureren.

Wat hebben we dan in handen? Metadata zijn data die nodig zijn om technologie haar werk te laten doen. De inhoud van een mail en de inhoud van een telefoongesprek zijn geen metadata, de ge-gevens die nodig zijn om die mail van afzender naar ontvanger te krijgen of de telefoonnummers, het tijdstip en de locatie van de zendmast zijn dat wel. De informatie op een webpagina of in een

app zijn geen metadata, het webadres en het tijdstip waarop je deze bezoekt zijn dat wel.

Het is november 2013, vijf maanden nadat Edward Snowden de wereld in zijn greep heeft gekregen door duizenden geheime NSA-documenten te lekken naar journalisten. Een van de lessen die we daaruit leren, is de enorme gretigheid waarmee de NSA en andere inlichtingendiensten metadata van miljarden burgers verzamelen.

Politici en inlichtingendiensten praten het binnenharken en analyseren van metadata goed door te benadrukken dat dan niet naar de inhoud wordt gekeken. 'Het recht op de bescherming van de persoonlijke levenssfeer [...] is slechts in beperkte mate in het geding,' zei toenmalig minister van Justitie Ernst Hirsch Ballin toen hij in 2009 de zogenoemde bewaarplicht verdedigde, een wet die regelde dat telecomproviders metadata van hun klanten moesten bewaren. 'Over de inhoud van communicatie wordt niets vastgelegd.'

Ook na Snowdens onthullingen benadrukken politici, inlichtingendiensten en opiniemakers dat het wel meeviel. Zo zegt president Barack Obama, nadat was gebleken dat de NSA de metadata van de telefoon van zo ongeveer iedere Amerikaan verzamelt: 'Niemand luistert mee als je belt. [...] Ze kijken niet naar namen en ze kijken niet naar de inhoud, maar doorzoeken dat wat metadata heet. Daar halen ze mogelijk informatie uit over mensen die betrokken zijn bij terrorisme.'

De Nederlandse AIVD zet na Snowdens onthullingen het volgende op zijn eigen site: 'Het vergaren van metadata betreft [...] een minder zware inbreuk op de privacy.' En Rob de Wijk, vooraanstaand defensie-expert en voorzitter van de Denktank Nationale Veiligheid, vertelt het *NOS Journaal* dat de zorgen over het verzamelen van metadata te wijten zijn aan '[...] onbekendheid met het fenomeen. Met metadata verzamelen op zich vind ik dat de privacy nog niet echt in het geding is. Dat gebeurt pas echt als je de diepte ingaat.'[53]

Gevoelsmatig zégt de inhoud van de communicatie ook veel meer dan de informatie over die communicatie. We zijn geneigd het prima

te vinden als de hele wereld weet dat wij onze partner dagelijks mailen, maar wat in die mailtjes staat, gaat niemand iets aan. De inhoud van onze communicatie is iets wat wij veel sneller zouden verbergen voor onbevoegden dan de metadata van die communicatie.

Een onterechte aanname.

In de vorige hoofdstukken werd al duidelijk hoeveel data er over ons verzameld worden en waar die naartoe stromen. We hebben gezien hoe moeilijk – en vaak zelfs onmogelijk – het is om onze datastromen te volgen. Wat we dan nog niet weten: waarom jagen overheden en bedrijven op onze data? Wat zeggen die gegevens over ons? Ons experiment met de metadata van Ton Siedsma geeft hier antwoord op.

Wat Siedsma's metadata over hem vertellen

Na een week levert Siedsma de metadata in die zijn app heeft geregistreerd. Eerst structureren we alles. We zetten de meer dan 15.000 datapunten – mails, locaties, telefoontjes en appjes – in chronologische volgorde. Van iedere keer dat Siedsma's telefoon contact legde met een zendmast, van iedere keer dat hij een e-mail stuurde of een site bezocht, kunnen we zien wanneer hij dat deed en waar hij zich tot op enkele meters nauwkeurig bevond.

Uit zijn bel- en e-mailverkeer kunnen we verder zijn sociale netwerk destilleren: met wie heeft hij veel contact, wie is belangrijk voor hem. En uit zijn browsegegevens kunnen we opmaken welke sites hij heeft bezocht en wat hij met zoekmachines probeerde te vinden (de zoekopdrachten zelf worden niet geregistreerd, maar de zoektermen staan wel in de URL, het internetadres, van de resultaten, bijvoorbeeld: www.google.nl/#?q=de_zoekterm_staat_dan_hier.) Van iedere e-mail kunnen we bovendien het onderwerp, de afzender en de ontvanger zien.

Siedsma's gestructureerde metadata analyseren we eerst zelf. Vervolgens delen we die met het iMinds-onderzoeksteam van de

Universiteit van Gent en met Mike Moolenaar, eigenaar van Risk & Security Experts en oud-medewerker bij een Nederlandse inlichtingendienst. De Gentse onderzoekers ontrafelen het sociale netwerk van Siedsma. Moolenaar bekijkt de data zoals een inlichtingendienst dat zou doen.

Na het samenvoegen van deze drie analyses maken wij een afspraak met Siedsma. Nerveus zit hij tegenover ons. Hij heeft niets te verbergen, niets illegaals in ieder geval. En hij weet dat wij héél veel over zijn privéleven hebben gevonden. Dit is wat zijn metadata over hem vertellen.

Ton Siedsma is begin twintig en nog niet zo lang afgestudeerd. Hij krijgt e-mails over studentenhuisvesting en bijbanen, op te maken uit de onderwerpregels en de afzenders. Hij maakt lange dagen, mede doordat hij elke dag lang in de trein zit. Vaak is hij niet voor acht uur 's avonds thuis. Eenmaal daar gaat het werk door tot ver in de avond, want er wordt tot laat druk met collega's gebeld en ge-e-maild.

Zijn vriendin heet Merel – haar achternaam mochten wij van Siedsma niet vermelden. Of ze samenwonen weten we niet zeker. Gemiddeld sturen ze elkaar honderd WhatsAppberichten per dag, vooral op momenten dat Siedsma de deur uit is. Voordat hij op Amsterdam Centraal in de trein stapt, belt Merel hem elke dag nog even op. Siedsma heeft een zus die Annemieke heet. Zij studeert nog: een van de mails gaat over haar scriptie, zo staat in de onderwerpregel.

Siedsma leest graag over sport op nu.nl, nrc.nl en volkskrant.nl. Hij is vooral geïnteresseerd in fietsen. Ook leest hij Scandinavische thrillers, althans daar zoekt hij naar op Google en Yahoo!. Hij heeft interesse in filosofie en religie. We vermoeden dat Siedsma christelijk is. Hij zoekt naar informatie over religiedeskundige Karen Armstrong, het evangelie van Thomas, 'de Messias boek middeleeuwen' en over symboliek in kerken en kathedralen.

Maar hij heeft ook een lichtere kant. Hij bekijkt YouTubefilm-pjes als *'jerry seinfeld sweatpants,'* 'brab guus meeuwis' en Rick Astley's *'never gonna give you up.'* Ook bekijkt hij een filmpje van de Brabantse realityster Roy Donders. Op internet leest hij over *'cats wearing tights,' 'disney princesses with beards'* en *'guitars replaced by dogs.'* Ook is hij op zoek naar een snuggie – een deken die je aan kunt trekken. Zijn oog is gevallen op de Batman Lounger Blanket With Sleeves.

Siedsma gebruikt drie e-mailadressen. Op zijn Hotmailadres ko-men alle aanbiedingen binnen. Dit adres gebruikt hij ook om me-een aantal kennissen te communiceren. Hij verstuurt zelf nauwelijks berichten vanuit dit adres. Hij heeft een tweede privé-e-mailadres Dat gebruikt hij deels voor werk en deels om met vrienden te com-municeren. En hij heeft een werkmailadres. Uit de data blijkt da Siedsma bij digitaleburgerrechtenorganisatie Bits of Freedom werkt Hij houdt zich daar vooral bezig met internationale handelsakkoor-den en onderhoudt daarover contact met het ministerie van Buiten-landse Zaken en enkele Kamerleden. Hij volgt de besluitvorming van de Europese Unie in Brussel op de voet. Daarnaast is hij geïnteres-seerd in opsporingsmethoden van politie en inlichtingendiensten We weten dat uit zijn mailverkeer en uit de dossiers die Siedsma bijhoudt op een afgesloten deel van de website van Bits of Freedom In sommige internetadressen die hij bezoekt, staan de namen van d dossiers. De dossiers gaan over internationale handelsverdragen, he parlement, de Wet Computercriminaliteit III en andere wetgeving Siedsma houdt ook de website van Bits of Freedom bij. We kunnen bijvoorbeeld terugvinden welke blogs hij heeft bewerkt.

Siedsma neemt in de onderzochte week actief deel aan een e-maildiscussie met zijn collega's met als onderwerp *'Van Delden must go.'* De mails gaan over Bert van Delden, de voorzitter van d CTIVD, de toezichthouder op de inlichtingendiensten AIVD en MIVD. Op 18 november verschijnt er een blog van Bits of Free-dom-directeur Ot van Daalen met daarin een oproep met dez strekking.

Gedurende de week is het nodige mailverkeer erop gericht een afspraak te maken met de assistent van VVD-Kamerlid Foort van Oosten en een zekere journalist Bart. Daarnaast heeft hij veel contact met aanbieders van antivirussoftware.

Ton Siedsma heeft relatief weinig contact met mensen buiten zijn werk. In zijn vrije tijd lijkt hij niet zo gek veel te doen. De werkmails komen tot laat in de avond binnen en hij beantwoordt ze vrijwel meteen. Ook surft hij veel naar nieuwssites en whatsappt hij met voor ons onbekenden. Doorgaans gaat hij tegen twaalf uur 's avonds naar bed, tenminste, dan vallen de digitale activiteiten stil. Alleen zijn smartphone geeft nog geregeld zijn locatie door: thuis.

Uit de socialenetwerkanalyse van zijn mailverkeer kunnen we verschillende groepen onderscheiden waar Siedsma deel van uitmaakt. Via zijn Hotmailaccount communiceert Siedsma met vrienden en kennissen. Thomas, Thijs en Jaap – hun achternamen mochten wij ook niet noemen – lijken de gangmakers van een grotere vriendengroep. Aan de mailadressen te zien, zijn het allemaal mannen. Ook loopt er een lijn naar een losstaande groep met als middelpunt ene 'Bert.' Wat dit voor groep is, wil Siedsma voor de buitenwereld verborgen houden: hij heeft ons gevraagd hierover niet te publiceren. Volgens hem is het karakter van deze groep een privéaangelegenheid.

Metadata zijn gedragsgegevens

Het experiment met Ton Siedsma maakt duidelijk dat metadata gaan over wie wij zijn, wat we doen en met wie wij omgaan. Daar is niks onpersoonlijks aan, zoals de term doet vermoeden en politici, inlichtingendiensten en opiniemakers beweerden. Ze vertellen bij uitstek iets over menselijk gedrag. In Siedsma's geval bleek dan ook alles aan de analyse te kloppen, behalve de observatie dat hij christelijk is.

Jaap-Henk Hoepman, universitair hoofddocent Technische Privacybescherming aan de Radboud Universiteit Nijmegen, bevestigt het intieme karakter van metadata. 'Weten wat iemand doet, zegt heel veel over wat iemand drijft. Als je iemand afluistert weet je niet zeker of diegene de waarheid spreekt. Maar metadata liegen niet, je ziet gewoon hoe iemand zich gedraagt.'

De patronen die uit metadata te halen zijn, kunnen veel zeggen over de inhoud van de communicatie, legt Matthijs Koot, expert op het gebied van IT-beveiliging en privacy bij beveiligingsbedrijf Madison Gurkha, ons uit. 'Als je geregeld belt met jeugdzorg of een psychiater, dan vertelt dat al iets over de inhoud van die communicatie. En er valt natuurlijk ook wel wat af te leiden van een telefoon die zich over een langere periode dag en nacht in een psychiatrische kliniek bevindt.'

'Metadata is de boodschap,' schreef de beroemde Amerikaanse onderzoeker Matt Blaze dan ook in technologietijdschrift *Wired*. 'Metadata vormen onze context. En die kunnen veel meer van ons blootleggen – zowel op individueel niveau als in groepen – dan de woorden die wij spreken.'[54]

Tot die conclusie kwam ook Pedro Cruz Villalón, de advocaat-generaal van het Europese Hof van Justitie. Cruz Villalón schree een pleidooi tegen de zogenoemde dataretentierichtlijn.[55] Deze om streden richtlijn verplichtte lidstaten van de Europese Unie o metadata van internet- en telefoniegebruik van alle Europese bu gers minstens een halfjaar op te slaan. In 2014 werd deze richtli door het Hof afgeschoten. Cruz Villalón schreef in zijn pleidooi d metadata tot een speciale categorie persoonlijke gegevens behor en dat die daarom ook als zodanig moeten worden behandeld. 'H gebruik van metadata,' schreef hij, 'maakt het mogelijk om een co pleet en accuraat beeld te creëren van iemands privé-identiteit.'

De organisatie waar Ton Siedsma voor werkt, Bits of Freedo heeft inmiddels besloten het verhullende woord 'metadata' n meer te gebruiken en consequent over 'gedragsgegevens' te sp ken. Wij gaan daar graag in mee, zeker na ons experiment.

Wat je met gedragsgegevens kunt

De analyse van gedragsgegevens is de afgelopen jaren een heus onderzoeksveld geworden. Zo gek is dat niet. Met onze gedragsgegevens worden onderzoekers, bedrijven en overheden in staat gesteld om mensen helemaal te leren kennen en om toekomstig gedrag te kunnen voorspellen. Gedragsgegevens zijn fantastisch onderzoeksmateriaal.

De beroemde Amerikaanse informaticus Alex Pentland heeft zelfs een veelzeggende titel aan deze nieuwe wetenschap gegeven: de sociale natuurkunde. Pentland gelooft heilig in de revolutie die de sociale natuurkunde teweeg zal brengen. 'Voor het eerst zullen we beschikken over de data die nodig zijn om onszelf echt te kennen en om te begrijpen hoe onze samenleving zich ontwikkelt,' schrijft hij in zijn boek *Social Physics* (2015).[56] Zijn optimisme kent geen grenzen: 'Over slechts een paar jaar kunnen we waarschijnlijk beschikken over ongelooflijk rijke data over het gedrag van de gehele mensheid – op een permanente basis.' Met de sociale natuurkunde streeft Pentland zo naar een 'computationele theorie van gedrag,' een 'wiskundige verklaring van de redenen waarom de samenleving reageert zoals ze reageert.' En Pentland is een invloedrijk man. Hij is hoogleraar aan het Massachusetts Institute of Technology, lid van het World Economic Forum en door *Time Magazine* een van de belangrijkste denkers van de eenentwintigste eeuw genoemd.

Zijn ambities reiken dan ook ver. Pentland meent dat met de nieuwe methoden om grote hoeveelheden data te analyseren niet alleen menselijk gedrag perfect gemeten kan worden, net als energie en beweging, maar ook kan worden voorspeld en zelfs gestuurd. Het doel is 'om betere systemen te ontwikkelen' en 'de toekomst exacter [te] kunnen plannen,' met samenlevingen als 'levende laboratoria.' Dit is cruciaal. Aan de sociale natuurkunde ligt een ultiem maakbaarheidsideaal ten grondslag.

'In dit boek laat ik zien hoe we een samenleving kunnen gaan opbouwen die beter in staat is om beurskrachs, etnisch en religieus geweld, politieke impasses, wijdverspreide corruptie en gevaarlijke machtsconcentraties te vermijden.' Sociale natuurkunde stelt ons volgens Pentland in staat om de wereld voorgoed te verbeteren.

Anonimiteit bestaat niet meer

Een nobel streven. Wij zijn vooral benieuwd wat de analyse van gedragsgegevens nu precies over ons onthult. Veel bedrijven en overheden die gedragsgegevens analyseren en gebruiken, beweren bijvoorbeeld dat dit anonieme data zijn. Zodra ze je data ontvangen, verwijderen ze alle gegevens die direct tot een persoon zijn te herleiden. Een belofte ter geruststelling: deze data gaan straks niet meer over jou.

Dat niets minder waar is, bleek uit een studie van het Massachusetts Institute of Technology die begin 2015 verscheen, waarvan Alex Pentland zelf medeauteur was. De onderzoekers analyseerden een paar miljoen creditcardbetalingen van enkele tienduizenden shoppers. Alle namen waren verwijderd. Door te kijken naar bestedingspatronen, tijdstippen en locaties van winkels lukte het de onderzoekers 90 procent van de shoppers tot unieke personen te herleiden.[57]

Combineer je de ene database met een andere, dan kun je bizarre inzichten krijgen. In 2013 gaf de gemeente New York na een openbaarheidsverzoek een enorme dataset vrij van alle taxiritten uit datzelfde jaar. Daarin was identificerende informatie over chauffeurs en taxi's versleuteld en informatie over ritprijs, instaplocatie en bestemming niet. Een slimme hacker kwam er al snel achter dat de namen van de chauffeurs niet goed versleuteld waren. Zo kon hij per taxichauffeur zien waar die allemaal was geweest dat jaar en wat hij verdiend had.

Een andere onderzoeker ging met de taxidata aan de slag om uit te vogelen of bekende Amerikanen hun chauffeurs fatsoenlijke fooien (minimaal 10 procent) geven. Op roddelsites zocht hij naar

foto's van bijvoorbeeld beroemde acteurs die op dat moment in een taxi stappen. Vaak stond in de data van dat fotobestand hoe laat die foto werd genomen en soms ook waar. Daarnaast was op sommige foto's het taxinummer te zien. Door die data te vergelijken met de taxidataset kon hij achterhalen waar de acteurs naartoe waren gegaan en hoeveel ze hadden betaald voor hun rit. Actrice Jessica Alba bleek bijzonder gierig als het op fooien aankwam.[58]

Ook gevoeligere kenmerken – zoals gezondheid, of politieke en religieuze overtuiging – kunnen uit ogenschijnlijk betekenisloze databestanden gehaald worden. Zo namen onderzoekers van de Stanforduniversiteit likes op Facebook onder de loep.[59] Aan de hand van 58.466 Facebookgebruikers die gemiddeld 170 keer hadden geliket, kwamen zij tot de volgende conclusie: Facebook-likes kunnen, in combinatie met statistiek, gebruikt worden om automatisch en accuraat een aantal zeer individuele eigenschappen te voorspellen. Namelijk: seksuele geaardheid, etniciteit, religieuze en politieke opvattingen, intelligentie, geluk, gebruik van verslavende middelen, leeftijd, geslacht en of de ouders van de liker gescheiden zijn.

Likes kunnen ook onze sociale relaties gedetailleerd in kaart brengen. Het Digital Methods Initiative, de onderzoeksgroep die hielp bij ons trackeronderzoek, gebruikte ze na de moorden van Anders Breivik om een contra-jihadistisch netwerk bloot te leggen. Dit netwerk bestaat uit verschillende groepen en individuen die zich verzetten tegen wat in hun ogen de 'islamisering' van de wereld is. Door onder andere onderlinge likes te volgen, konden de onderzoekers nagaan wie hierbinnen belangrijk is, naar wie wordt geluisterd en hoe verschillende individuen en groepen zich tot elkaar verhouden.

Voorspellend politiewerk in Nederland

De nieuwe wetenschap van gedragsgegevens maakt het niet alleen
mogelijk om mensen te doorgronden, maar ook om hun gedrag
te voorspellen. Een van de fascinerendste ontwikkelingen op dit
gebied is het zogenoemde *predictive policing*, voorspellend politie-
werk. Het idee dat opsporingsdiensten door grootschalig data te
verzamelen patronen in menselijk gedrag kunnen herkennen die
kunnen leiden tot criminaliteit. Om dan, nog voor een misdaad is
gepleegd, in te kunnen grijpen.

De Amerikanen lopen – zoals wel vaker – voorop op dit gebied
Zo gingen in 2008 de politiediensten van Los Angeles en Santa
Cruz een samenwerkingsverband aan met de universiteiten van
Californië en Santa Clara. Daaruit ontstond het programma Pred
Pol, dat inmiddels in verschillende grote steden in de Verenigde
Staten gebruikt wordt. Het programma werkt volgens de zoge
noemde *near-repeat*-methode, gebaseerd op de manier waarme
naschokken van een aardbeving berekend kunnen worden. Al
ergens een misdaad gepleegd wordt – zoals een schietpartij –, i
de kans groot dat er kort daarna weer een misdaad gepleegd za
worden – zoals een vergelding voor die schietpartij. In Duitslan
en Zwitserland wordt inmiddels met een vergelijkbaar systeem
gewerkt, dat de naam Precops draagt.

Hoe staat het in Nederland met predictive policing? Met onde
zoeksassistente Anne Schepers lezen we talloze beleidsstukken e
spreken we verschillende politiemedewerkers.[60] We ontdekken d
ook hier stappen worden gezet in voorspellend politiewerk: d
Nederlandse politie experimenteert met data-analyse om misdri
ven te voorkomen.

Tekenend voor de hooggespannen verwachtingen is een begi
2015 uitgelekt visiedocument van het Korps landelijke politi
diensten (tegenwoordig Nationale Politie). In het document, g
schreven in 2011, bezingen de auteurs een landelijk camera- e

sensorennetwerk als toekomst van de criminaliteitsbestrijding in Nederland. Door camera's en sensoren van winkels, kantoren en openbaarvervoersbedrijven aan elkaar te koppelen, kan de politie een zo volledig mogelijk overzicht krijgen van de openbare ruimte. Op die manier is de politie, aldus de auteurs, in staat om 'gebeurtenissen in de nabije toekomst te voorspellen' om vervolgens 'proactief te acteren.'

Er liggen nog meer plannen klaar bij de Nationale Politie. Rutger Rienks, hoofd van de afdeling Business Intelligence bij de Nationale Politie, beschrijft ze in zijn boek *Predictive policing: kansen voor een veiligere toekomst.*[61] De voorwaarde voor predictive policing, aldus Rienks, is het grootschalig inzamelen van data. Alleen door daar experimenten mee te doen, meent Rienks, kan nagegaan worden welke gegevens nodig zijn voor het voorspellen van criminaliteit.

Rienks pleit zo voor het volgen van het woon-werkverkeer van alle Nederlanders. Want als camera's weten welke route je iedere dag naar je werk aflegt, merkt de technologie het op wanneer je daarvan afwijkt. Neem je een afslag richting een verlaten bedrijventerrein, dan kan dat een aanwijzing zijn dat je een drugscrimineel bent, stelt Rienks. En als je camera's ophangt in een winkelstraat, kun je een potentiële zakkenroller volgen door middel van gezichtsherkenning en zijn gedrag in de gaten houden. Rienks droomt ook over camera's die aan samentrekkingen in het gezicht kunnen zien of iemand agressief gaat worden. Ook dat – of eigenlijk júíst dat – is predictive policing: een constante monitoring van de samenleving, waarbij afwijkend gedrag als voorbode van criminaliteit wordt gezien.

Nog los van de evidente schending van het recht op privacy en de wettelijke onschuldpresumptie – het gegeven dat je onschuldig bent tot het moment dat je schuld is bewezen –, zijn de politieplannen vooralsnog toekomstmuziek. Binnen de dienst zijn wel talloze enthousiaste pleitbezorgers van predictive policing te vinden.

Dat merkt Schepers als ze op bezoek gaat bij Dick Willems, d ontwerper van het Criminaliteits Anticipatie Systeem (CAS), da door de Amsterdamse politie gebruikt wordt om straatroven e woninginbraken te voorspellen. Het flexteam, bestaande uit agen ten die overal in de stad inzetbaar zijn, baseert er sinds 2013 zij surveillanceroutes op.

Hoe CAS werkt? Politiemedewerkers weten waar veel crimina liteit plaatsvindt, vertelt Willems. 'Ze kunnen bijvoorbeeld he aantal woninginbraken visualiseren op de kaart van Amsterdam zodat je een soort vlekkenkaart krijgt. Daarop is te zien op welk plekken in het verleden veel inbraken hebben plaatsgevonden.' Al je weet waar in het verleden veel criminaliteit plaatsvond, kun j dit met CAS berekenen voor het heden. Het systeem voorspel volgens Willems zo'n 40 procent van de woninginbraken en 6 procent van de straatroven correct. CAS is dan ook in trek bij d Nationale Politie: er zijn verschillende pilots gehouden in politie regio's in Nederland.

Nudgen door de overheid

Overheden en publieke organisaties maken in toenemende mat gebruik van dataverzamelingen om ons gedrag te sturen. Dit stu ren door overheden heet *nudging*. In 2008 bestormde dat begri het wereldtoneel toen de Amerikaanse onderzoekers Cass Sun stein en Richard Thaler hun bestseller *Nudge: Improving Decision About Health, Wealth and Happiness* publiceerden.[62] Hun stellin was dat overheden en bedrijven mensen niet moesten dwinge bepaald gedrag te laten, maar mensen moesten verleiden.

Een van hun voorbeelden is de aanpak van obesitas onder jon geren. In Amerika eten veel scholieren hun lunch in een schoo kantine. Ongezond eten verbieden heeft weinig zin: dan neme jongeren het zelf mee. Volgens Sunstein en Thaler was het daaron zinniger het aanbod in de kantine anders in te delen: het gezond

voedsel vooraan, het ongezonde op een minder zichtbare plek. Een aantal studies toonde aan dat meer jongeren dan, vaak onbewust, voor het gezonde voedsel kozen.

Dergelijke beïnvloedingstechnieken kunnen effectiever worden als je veel data tot je beschikking hebt en die kunt analyseren. Zo geven persoons- en gedragsgegevens beleidsmakers inzicht in het gedrag van mensen zodat ze sneller kunnen zien waar ze moeten ingrijpen én zorgen deze ervoor dat ze het effect kunnen meten van deze interventie. De Belastingdienst heeft zelfs een speciale nudge-afdeling in het leven geroepen, het Team Gedragsverandering, dat op allerlei manieren probeert om onder andere 'chronische uitstellers' op tijd hun belasting te laten betalen.[63] En ons ministerie van Infrastructuur en Milieu probeert automobilisten te verleiden het openbaar vervoer te nemen. Op drukke wegen worden de kentekens van passerende auto's gescand, bijvoorbeeld in de ochtend- en avondspits. Vervolgens krijgt een aantal automobilisten een aanbieding per post om goedkoper gebruik te maken van het openbaar vervoer.

De Amerikaanse socioloog James B. Rule noemt dergelijke interventies 'sociale beheersing.' Hij schrijft: 'Sociale beheersing verwijst naar een verzameling processen die het juiste soort gedrag aanmoedigt of ongewenst gedrag afraadt.' Deze sociale beheersing kent volgens Rule een wijd spectrum aan toepassingen, van 'vriendelijk tot repressief.'[64] Van het bevorderen van publieke gezondheidszorg – door nudging – tot het identificeren van potentiële terroristen – door de analyse van digitale gedragsgegevens.

'Het is onmogelijk om "goed" gedrag te stimuleren en het tegenovergestelde te ontmoedigen zonder te weten hoe die personen zich in het verleden hebben gedragen,' analyseert Rule verder. 'Dit leidt tot de dorst van publieke en private organisaties om de data van de mensen waar ze mee te maken hebben te creëren, analyseren, delen en op te slaan.'

Sociale beheersbaarheid is geen nieuwe ontwikkeling. Overheden hebben er altijd alles aan gedaan burgers te sturen, variërend

van het invoeren van wetten en regels tot het met geweld afdwingen van gedrag, en bedrijven zijn er altijd op gericht geweest klanten te verleiden. Beide hebben daar bovendien altijd informatie over individuen voor nodig gehad.

Nieuw is wel dat de technologie en wetenschap overheden en bedrijven in staat stellen zowel het gedrag van groepen mensen te analyseren en te beïnvloeden, als het menselijk gedrag van individuen te doorgronden en te sturen.

Hoe adverteerders dit in de praktijk doen

Op weinig plekken zie je deze ontwikkeling zo duidelijk terug als in de advertentiewereld. Alleen wil geen enkele adverteerder die wij benaderen ons erover vertellen. Behalve wiskundige en sociaal psycholoog Maurits Kaptein. Hij zal ons de geheimen van de online beïnvloeding uitleggen.

Kaptein vertelt dat de dominante theorieën over menselijk gedrag grote beperkingen kennen. Als voorbeeld noemt hij de beruchte experimenten van Stanley Milgram. Deze Amerikaanse sociaal psycholoog liet in de jaren zestig zien dat mensen heel ver konden gaan in het uitvoeren van orders. Sommige proefpersonen waren bereid andere proefpersonen een potentieel dodelijke schok van 450 volt toe te dienen als dat hun werd opgedragen door een man in een witte jas. De les van Milgram: wij mensen gehoorzamen mensen die wij een zekere autoriteit toedichten.

De inzichten van Milgram vinden vanaf de jaren zestig gretig aftrek in de reclamewereld. Want als je weet waar mensen gevoelig voor zijn, kun je daarop inspelen en zo hun gedrag beïnvloeden. Dus beveelt sindsdien een knappe vrouw dagcrème aan en verkoopt een man in een witte jas tandpasta.

Dus ja, het autoriteitsargument werkt, zegt Kaptein. 'Als je goed kijkt naar de experimenten, blijkt inderdaad dat mensen gemid-

deld genomen gevoelig zijn voor autoriteit. Maar: 35 procent van Milgrams proefpersonen was daar niet gevoelig voor.'

Met andere woorden: het autoriteitsargument geldt alleen voor groepen en zegt helemaal niets over de individuen binnen die groepen. En dat geldt voor alle sociaalwetenschappelijke theorieën over gedrag, meent Kaptein.

Het interessante is, zegt de onderzoeker, dat sinds het bestaan van internet wél naar het individueel niveau kan worden gekeken. 'Het internet is de beste telescoop op menselijk gedrag dat ooit gemaakt is. Online kunnen we voor het eerst op heel grote schaal het werkelijke gedrag van heel veel mensen observeren. Daar kunnen we van leren en zo toekomstig gedrag beter voorspellen dan ooit.'

In 2011 zette Kaptein met een collega van de Stanforduniversiteit bij wijze van experiment een online boekwinkel op.[65] De twee vroegen sitebezoekers verschillende boeken te bekijken en te evalueren. De onderzoekers testten ondertussen verschillende beïnvloedingsstrategieën. Het ene boek kreeg een autoriteitsargument mee ('Boek van het jaar volgens Matthijs van Nieuwkerk'), terwijl het andere boek werd gepitcht volgens de zogenoemde *social proof*-strategie ('Dit is het populairste boek onder jouw Facebookvrienden'). Ook werden sommige boeken met korting aangeboden of als bestseller gepresenteerd.

De bezoekers bleken nogal verschillend op de strategieën te reageren. Wat werkte voor de een, werkte juist niet voor de ander. Doordat Kaptein realtime de strategieën kon aanpassen, wist hij de effectiviteit van een boekaanbeveling met 30 tot 40 procent te verhogen. 'Wij konden op een gegeven moment heel goed voorspellen hoe iemand zou reageren.'

Kaptein ontwikkelde naar aanleiding van het experiment het idee van '*persuasion profiles*,' beïnvloedingsprofielen die per persoon verschillen. Als je weet voor welke verkoopargumenten iemand gevoelig is, weet je precies op welk knopje je moet drukken om de kans te vergroten dat iemand een product koopt.

Kaptein verdeelt zijn tijd nu tussen de wetenschap – hij is docent statistiek aan de Universiteit van Tilburg – en zijn eigen bedrijf, Science Rockstars, dat klanten als UPC, *nrc.next* en ING bedient. Een andere klant is cosmeticawinkel Rituals. Kaptein: 'In hun webshop zijn sommige producten in de aanbieding en andere niet. Bij sommige producten wordt vermeld dat ze veel verkocht worden, bij andere niet. Wij kunnen zien dat sommige bezoekers niet graag een populair product kopen, maar liever iets exclusiefs. Als ik dat weet, kan ik dat heel simpel aanpassen en er de volgende keer niet meer bij vertellen dat het een vaak verkocht product is.'

Kaptein meet dus hoe de bezoekers op verschillende verkoopstrategieën reageren en past de aanbevelingen aan op het moment dat de site door de computer van de bezoeker wordt herladen. 'De mooie manier van zeggen is dat ik realtime de pagina van de webshop zo opbouw dat hij het meeste overeenkomt met jouw voorkeuren. De platte manier van zeggen is dat ik er zo voor zorg dat je de meeste producten koopt.'

Kaptein vertelt dat zijn bedrijf alleen het gedrag van bezoekers op één bepaalde site analyseert en dat de klanten niet op andere sites gevolgd worden. Maar je hoeft niet over heel veel fantasie te beschikken om te zien dat persuasion profiles uit veel meer kunnen bestaan dan of je wel of niet gevoelig bent voor korting of het autoriteitsargument. Denk alleen al aan de informatie over online en offline gedrag en demografische gegevens die datahandelaren over ons in huis hebben, of wat Facebook en Google over ons weten.

Gedragsgegevens worden verzameld om profielen van ons te maken en om ons vervolgens zo gericht mogelijk te benaderen en nog liever: ons toekomstig gedrag te voorspellen. *Behavioral targeting* heet dit en het is de Heilige Graal van de advertentiewereld. En de zoektocht naar die Heilige Graal is een harde wetenschap geworden.

'De briljantste geesten van mijn generatie denken na over hoe ze mensen het best op advertenties kunnen laten klikken.' Wa

getekend: Jeff Hammerbacher, een oud-Facebookmedewerker. Hij doet deze uitspraak in een artikel in *Business Week* uit 2011 over zogenoemde '*wants*,' wiskundigen die in dienst van technologie- en digitaleadvertentiebedrijven uitrekenen hoe zij bezoekers zo vaak en zo snel mogelijk op een advertentie kunnen laten klikken.[66] De term 'want' is een afgeleide van '*quant*,' de mathematici die voor bedrijven op Wall Street geavanceerde algoritmes bouwen die grote hoeveelheden economische data analyseren en zo automatisch in aandelen en opties handelen. Wants doen in principe hetzelfde, maar dan met consumentendata. Zoals de auteur van het *Business Week*-artikel treffend schrijft: 'Zij snuffelen rond in data, jagen op trends en bedenken formules die de juiste advertentie aan de juiste persoon voorschotelt. Wants meten de persoonlijkheidstypes van klanten, bepalen hun begeerte voor bepaalde producten en bepalen wat mensen motiveert om op een advertentie te reageren.'

Maurits Kaptein herkent deze trend. 'Alle slimme bètajongetjes worden *data scientist* bij een technologiebedrijf. Een jongen waar ik veel mee samenwerkte, een briljant wiskundige, zit bij Facebook. Hij stond voor de keuze om of voor de universiteit te gaan werken, waar hij les moest geven en niet heel veel betaald kreeg, of bij Facebook, waar hij samen kon werken met een paar zeer goede onderzoekers, geen les hoeft te geven, vier keer zoveel betaald krijgt en toegang heeft tot enorme datasets. Er zit erg interessante wiskunde achter het werk dat hij doet, maar in essentie komt het neer op de vraag waar mensen op klikken.'

Pas op voor het surveillancekapitalisme

Nu kun je zeggen: ach, het zijn maar advertenties, waarom ons daar zo druk over maken? Volgens de Amerikaanse auteur Shoshana Zuboff omdat de werkwijze van hedendaagse technologiebedrijven niets minder is dan een nieuwe economische werke-

lijkheid: het 'surveillancekapitalisme.' Een vorm van kapitalisme waarbinnen geld wordt verdiend door de grootschalige surveillance van menselijk gedrag. Zuboff: 'We zien dat het kapitalisme onder onze ogen verandert: eerst profiteerde het kapitalisme van producten en diensten, toen van speculatie en nu van surveillance. De nieuwe productiemiddelen zijn niet de machines van weleer maar de technologieën die betekenis halen uit al die data.

'Het moederschip' van deze nieuwe economische logica Google. In een prikkelende analyse stelt Zuboff dat de meeste mensen het succes van dat bedrijf onterecht toeschrijven aan zijn advertentiemodel. Zij denkt dat het anders zit: 'Googles succes komt voort uit zijn vermogen om de toekomst te voorspellen – vooral de toekomst van gedrag.' Meer informatie over het gedrag van gebruikers leidt tot betere voorspellingen, wat weer leidt tot hogere inkomsten. De verzameling van gedragsgegevens zal daarom explosief toenemen, denkt Zuboff. Wie de meeste data heeft en het slimst kan analyseren, heeft de meeste waarde in handen.

Een van de grote verschillen met het klassiek kapitalisme – en de reden dat Zuboff zich er zo druk over maakt –, is de radicaal andere relatie tussen de 'kapitalisten' en de 'consumenten.' Voor een bedrijf als autofabrikant Ford hadden burgers en consumenten een totaal andere betekenis dan voor Google, Facebook en andere surveillancekapitalisten. Voor Ford waren wij potentiële klanten óf mogelijke werknemers van het bedrijf. Hoewel het absoluut geen perfect systeem was, schrijft Zuboff, was er wé een grote wederzijdse afhankelijkheid tussen de bedrijven en het volk. Google, Facebook en andere surveillancekapitalisten hebben hier fundamenteel mee gebroken, stelt Zuboff. In plaats van een mogelijke afnemer of eventuele toekomstige collega zijn wi nu vooral een bron waaruit getapt kan worden. 'Gebruikers zijn de bron van het ruwe materiaal dat een nieuw soort productieproces voedt.'

Dus: waar ligt de grens?

De nieuwe vormen van sociale beheersing, voortgestuwd door de mogelijkheden van de sociale natuurkunde, bieden veel kansen. De belofte voor ons, als burgers en consumenten, is dat wij diensten en producten kunnen verwachten die aansluiten op wie wij zijn en wat wij willen. Ons leven kan er een stuk gemakkelijker, efficiënter en prettiger op worden.

Zo zijn de kansen voor de gezondheidszorg evident. Het is aanlokkelijk om interventies op maat te ontwerpen waardoor mensen echt stoppen met roken, minder gaan drinken, beter gaan eten of meer bewegen. In sommige ontwikkelingslanden kijken hulporganisaties naar telefoondata om te zien of hun economische hulpprogramma's effectief zijn: als er meer activiteit is, kan dat wijzen op een groeiende economie.

De mogelijkheden lijken eindeloos. 'Menselijk gedrag is fascinerend complex,' vertelt directeur Hans Blokpoel van de Belastingdienst in zijn werkkamer in Den Haag. 'De Belastingdienst maakt een ontwikkeling door van het maken van keuzes op basis van feiten [data-analyse] in plaats van op meningen [van inspecteurs].'

Vroeger, legt Blokpoel uit, was het werk van de fiscus overzichtelijker. 'Rond 1960 werkten burgers in de buurt van waar zij woonden. De arts, de politieagent, de belastinginspecteur: zij kenden die mensen. Als je bij de bank kwam voor een lening, hoefde je echt geen legitimatiebewijs mee te nemen. Nu is alles anders. Er zijn open grenzen, mensen wonen en werken op verschillende plekken, er zijn 1,2 miljoen bedrijven, miljoenen zzp'ers, negenduizend grote bedrijven, tien miljoen belastingplichtigen en een groot deel van het economisch verkeer voltrekt zich digitaal.'

In die wereld is het onmogelijk om iedere belastingplichtige persoonlijk te kennen. 'Ik moet dus anders gaan prioriteren,' zegt Blokpoel. 'Gebruikmakend van data in plaats van handwerk.' Hij noemt dit: 'informatiegestuurde, subjectgerichte handhavingsregie.' In gewonemensentaal: het analyseren van de enorme bakken persoonlijke gegevens om ervoor te zorgen dat iedere belastingplichtige belasting betaalt. Zijn slogan: 'Iedere belastingplichtige de behandeling geven die hij verdient.'

Blokpoel geeft een voorbeeld van waar dit in de nabije toekomst tot kan leiden: 'Als jij altijd op tijd je aangifte hebt gedaan, dan kan dat betekenen dat wij jou op onze site de mogelijkheid geven een betalingsregeling af te sluiten. Bij iemand die wij al twee keer zijn tegengekomen in een crimineel netwerk, doen we dat niet.'

Met trots vertelt Blokpoel dat er iemand voor hem werkt 'met groen haar,' die met andere bèta's – natuurkundigen, wiskundigen, sterrenkundigen – een nieuwe eenheid binnen de Belastingdienst vormt die de gegevens over Nederlandse burgers doorvlooit. Zij hebben een systeem gebouwd waarbij realtime enkele honderdduizenden notoire wanbetalers – burgers en bedrijven – in de gaten worden gehouden.

Als je netjes je belastingschuld betaalt, legt Blokpoel uit, is er niets aan de hand. Als je die rekening structureel níét vereffent, wordt het een ander verhaal. Dan kom je in die database terecht met andere notoire wanbetalers. Ontvang je vervolgens een erfenis, koop je een nieuwe auto, heb je een nieuwe baan: houd er dan rekening mee dat die informatie direct een alarm af doet gaan bij de Big Data-analisten van de fiscus en je gemaand wordt die schuld zo snel mogelijk te betalen. Dit noemt de Belastingdienst 'dynamisch monitoren.' Blokpoel: 'Alle normale maatregelen – herinneringen, aanmaningen – zijn dan al gepasseerd. Dus is het tijd voor een wat steviger aanpak.'

Ook richten Blokpoel en zijn team van analisten zich op *profi-ling*: zij zoeken in de databases naar patronen in het gedrag van groepen belastingbetalers. Zoals: welke factoren hangen samen met het verkeerd invullen van de inkomstenbelasting? 'Daar gaan we volkomen blanco in,' zegt Blokpoel. 'En dan blijken er factoren te zijn die een sterke correlatie hebben met een aangifte die niet klopt. Dan zou het dus zo kunnen zijn – en dit is een puur hypo

thetisch voorbeeld – dat als jij in een grijze Golf rijdt, de kans groot is dat je een aangifte doet waar iets mis mee is. Of dat mensen die in februari zijn geboren meer fouten maken. De volgende vraag is dan: Wat gaan we met die informatie doen? Welke behandeling gaan we deze mensen geven?'

Een niet-hypothetisch voorbeeld: uit de analyse van zijn team is gebleken dat individuen die in scheiding liggen meer fouten maken in hun aangifte. 'Logisch,' zegt Blokpoel. 'Scheiden is complex. Vroeger zou de instinctieve reactie bij de dienst zijn: we moeten die aangiftes beter gaan controleren. Nu benaderen we die groep vooraf. We schrijven ze een brief waarin we zeggen: mensen in uw situatie maken vaak fouten. Wat blijkt? Afhankelijk van de groep worden er dankzij deze brief 30 tot 70 procent minder fouten gemaakt. Een doorslaggevend succes.'

'Mijn missie is gedragsverandering,' vat Blokpoel samen. 'Zo krijg je uiteindelijk een maatschappij waarin ik wil leven. Een overheid die het lichtst mogelijke instrument inzet om mij ergens op te wijzen. En die zelf vaststelt of dat gerechtvaardigd is.'

Dat is nogal wat. En het roept direct de vraag op: waar ligt voor de Belastingdienst de grens? Stel je voor, vragen we, dat er op een gegeven moment een sterke correlatie wordt gevonden tussen het maken van fouten in de inkomstenbelasting en bijvoorbeeld iemands alcoholconsumptie of zoekgedrag op Google, kun je die inzichten dan gebruiken? 'Precies om die reden,' antwoordt Blokpoel, 'heb ik een veiligheidsventiel ingebouwd. Wij gebruiken voor het opstellen van risicoprofielen alleen gegevens die wij al in huis hebben. Alcoholconsumptie of zoekgedrag zijn geen onderdeel van de fiscale informatie die wij al hebben.' Want: 'Ik vind dat we eerst maar eens die maatschappelijke discussie moeten voeren. Tot die tijd doe ik niets anders dan het slimmer gebruiken van de gegevens die wij altijd al hadden. Er zijn heel veel mogelijkheden waarvan mijn datamensen weten dat het een *no-go area* is.'

Het zou dus wel kunnen dat dit veiligheidsventiel op een gegeven moment verdwijnt?

'Er zijn nog zo veel winstmogelijkheden in het beter gebruiken van gegevens die wij al hebben, dat ik nu geen enkele noodzaak heb om nieuwe gegevens te gebruiken.'

Met andere woorden: Blokpoel laat de mogelijkheid open.

We horen Blokpoel aan, lezen de positieve verhalen over de mogelijkheden van Big Data en kunnen er toch niet héél enthousias van worden. Er wringt iets.

Als wij als samenleving de sociale natuurkunde verder omar men, is er geen natuurlijke grens meer aan de verzameling e analyse van onze gedragsgegevens. Verzekeraars zijn nu aan he experimenteren met armbanden die bijhouden wat de hartslag e het calorieverbruik is van verzekerden die joggen. Wat weerhoud ze om dan ook het aantal uren slaap per nacht en hoe vaak ieman seks heeft in de week te meten? Om vervolgens een uitvoerig analyse van het gezondheidspeil van iemands sociale netwerk, zij inkomen, zijn hobby's en familierelaties te maken? Als je je al overheid of bedrijf eenmaal hebt voorgenomen om het gedrag va individuen te doorgronden, dan zijn de mogelijkheden tegenwoo dig – letterlijk – oneindig. En de gevolgen voor burgers en consu menten niet te overzien.

'In feite krijgt iedere burger een rapportcijfer.'[67]

– HOOGLERAAR STAATS- EN BESTUURSRECHT
MARGRIET OVERKLEEFT-VERBURG

'Vervang je actieve politiek en dynamisch rechtsdenken door algoritmes die een paar private clubs ooit ondemocratisch in elkaar hebben geknutseld, dan ben je niet alleen de politiek, maar ook het recht kwijt, en de levende moraal. En uiteindelijk de toekomst.'[68]

– PUBLICIST MAXIM FEBRUARI

5

Autonomie en democratie

Waarom privacy over veel meer gaat dan persoonsgegevens

Erik Pas heeft haast. Zijn vlucht van Amsterdam naar Los Angeles vertrekt om negen uur 's ochtends en hij wil nog even roken. Als hij daarmee klaar is, spoedt hij zich naar de gate. Vlak voordat hij zijn handbagage op de band zet, nemen twee mannen hem apart. Ze introduceren zichzelf als Amerikaanse *air marshalls*. Terwijl passagiers verderop hun zakken legen en riemen afdoen, schieten de twee vragen op hem af.

'Waar ga je naartoe?' ('Los Angeles.')

'Wat ga je daar doen?' ('Zaken.')

'Waar heb je je ESTA [document om Amerika binnen te komen] ingevuld?' ('Thuis.')

'Wanneer heb je dat gedaan?' ('Afgelopen maandag.')

'Heb je dat zelf gedaan?' ('Even nadenken... ja.')

Dan worden de air marshalls iets dwingender:

'Je antwoorden kloppen niet. Je was afgelopen maandag in Jordanië.' ('Nee.')

'In welke landen ben je de afgelopen jaren geweest?' ('Nou eens kijken...')

'Ben je weleens in Irak geweest?' ('Nee.')

'Afghanistan?' ('Nee.')

'Syrië?' ('Nee.')

'Jordanië?' ('Nee.')

Een stilte. En dan: 'Je was wél in Jordanië. Ben je op doorreis?' ('Nee, ik ben echt nog nooit in Jordanië geweest.')

'Mogen we je iPhone zien?' ('Ja.')

'Mogen we je iPad zien?' ('Ja.')
'Kun je je laptop even aanzetten?' ('Oké.')
'We willen je nog een keer fouilleren.' ('Goed.')
De air marshalls schrijven alle antwoorden op. Pas mag gaan.

Na elf uur vliegen komt hij aan in Los Angeles. Als het zijn beurt is bij de douane, roept de beambte er versterking bij. Twee bewapende agenten nemen Pas mee naar een wachtkamer.

Hij vraagt of hij iemand mag bellen.

'U mag voorlopig even niets meer,' luidt het antwoord.

Even later stappen twee agenten de kamer binnen en beginnen aan een verhoor.

'Met wie heb je een afspraak?'
'Waar en wanneer heb je die afspraken?'
'In welke landen ben je allemaal geweest?'
'Ben je ook in het Midden-Oosten geweest?'
'Welke socialemedia-accounts heb je?
'Waar verblijf je?'
'Wie zijn je ouders?'

Het vragenvuur houdt 45 minuten aan. Alles wordt opgeschreven. Dan mag Pas naar buiten. Hij haalt zijn huurauto op en vertrekt naar het appartement dat hij heeft geboekt. Hij is net tien minuten binnen als er wordt aangebeld. Twee agenten staan voor de deur. Ze willen weten wie hij is en waar hij vandaan komt. Geduldig legt Pas uit dat hij net drie kwartier is ondervraagd op het vliegveld en dat hij mocht gaan. De agenten schrijven iets in hun notitieboekje, bedanken hem en zeggen hem vriendelijk gedag.

Het verhaal van Erik Pas vinden we bij toeval in het voorjaar van 2015. In *De Telegraaf* staat een klein bericht over zijn reis naar Amerika.[69] We weten meteen dat we hem moeten spreken: zijn verhaal staat voor iets groters.

Privacy gaat over ons allemaal

Toen wij ons begonnen te verdiepen in privacy en surveillance, bekeken wij deze thema's nog door een beperkte bril. We zagen privacy als iets persoonlijks, als een individuele waarde die geschonden kan worden. In die visie draait privacybescherming om controle over de eigen data. Privacywetten dienen als wapens tegen surveillance door de overheid en het bedrijfsleven. De uitspraak 'ik heb niets te verbergen' past bij deze visie, omdat het gaat over een 'ik' die iets te verbergen heeft.

En ja, privacy *is* ook een individueel recht. Maar een van de belangrijkste inzichten die wij tijdens het onderzoek voor dit boek opdeden, is dat privacy niet alleen over onszelf, maar ook over anderen gaat. Privacy beschermt niet iedereen afzonderlijk, maar ons allemaal. Surveillance heeft niet alleen gevolgen voor individuen, maar is van invloed op de hele samenleving.

Tot nu toe ging deze zoektocht over de jacht op onze persoonlijke en gedragsgegevens. We lieten zien hoe onze data via de apps op onze smartphones en de websites die wij bezoeken terechtkomen bij heel veel partijen. We beschreven de fundamentele beveiligingsrisico's van de apparaten, systemen en sites waar wij onze data – bewust of onbewust – aan toevertrouwen. We zoomden in op de wijze waarop onze gegevens rondzwerven bij de Nederlandse overheid, hoe commerciële partijen als Google, Facebook en datahandelaren met onze data omgaan, en hoe bedrijven en overheden onze gegevens naar hartenlust uitwisselen. In het vorige hoofdstuk beschreven we ten slotte waar die enorme honger naar onze gedragsgegevens vandaan komt en wat de analyse ervan over ons allemaal – als individu en als groep – onthult. Een van de belangrijkste conclusies tot zover is dat burgers en consumenten nagenoeg machteloos staan tegenover de enorme krachten achter de datahonger.

Nu is het moment aangebroken om onze blik te verplaatsen

naar de gevolgen hiervan voor de hele samenleving. In toenemende mate worden er beslissingen over en voor ons genomen zonder dat wij het zelf doorhebben en zonder dat wij er enige invloed op kunnen uitoefenen. De afgelopen jaren hebben interessante denkers en goede journalisten laten zien dat dit gebruik van persoons- en gedragsgegevens door overheden en bedrijven serieuze risico's kunnen vormen voor enkele fundamentele democratische waarden. Daarmee zijn wij aangekomen bij het sluitstuk van onze zoektocht. Omdat de risico's waar wij het over zullen hebben nog niet altijd even goed zichtbaar zijn, heeft dit deel een iets hypothetischer karakter dan het voorgaande; we zien alleen nog maar de rimpelingen. Toch vormt dit voor ons de kern van ons onderzoek. Wat wij hier beschrijven, is een toekomst die nadrukkelijk op onze deur klopt. Vooral de analyse van grote hoeveelheden data – vaak aangeduid met de parapluterm Big Data – en het geautomatiseerde karakter ervan, zetten deze waarden onder druk. Het gaat dan om waarden als een *onvoorwaardelijk burgerschap*, de *onschuldpresumptie*, het *non-discriminatiebeginsel*, *autonomie*, *solidariteit* en *democratie*.

Van iedereen een profiel

Een van de denkers die onze ideeën hierover heeft gevormd, is de Canadese socioloog David Lyon. Hij was met zijn ideeën over de aard van surveillance zijn tijd ver vooruit. Toen de meeste mensen het nog over Big Brother hadden, sprak hij al over *social sorting*.

Social sorting is, in zijn definitie uit 2003, het sorteren van mensen op basis van hun gegevens.

Het vergaren, analyseren en gebruiken van persoonlijke gegevens heeft volgens Lyon altijd dit ene onderliggende doel.[70] Surveillance wordt zo – bot gezegd – ingezet om de 'goeden' van de 'kwaden' te onderscheiden en daarmee risico's te voorkomen of kansen te benutten.

Die risico's gaan vaak over veiligheid: kunnen we terroristen, criminelen en fraudeurs herkennen en stoppen? En die risico's gaan over geld. Welke klant zal ons winst opleveren en welke leidt tot verlies? Wie zal op een advertentie klikken en wie is onze aandacht niet waard?

Om dat onderscheid te kunnen maken, worden er door overheden en bedrijven profielen gemaakt. Meestal werkt dat als volgt. Er worden gedragsgegevens van heel veel mensen verzameld. Vervolgens wordt naar specifieke groepen gekeken. Hoe reist een terrorist? Hoe betaalt hij zijn ticket? Welke bestemmingen doet hij doorgaans aan? Heeft hij bepaalde maaltijdvoorkeuren? Reist hij alleen of in groepen? Als er een beeld bestaat van wat terroristisch gedrag zou kunnen zijn, kun je van alle mensen uitrekenen in hoeverre hun gedrag lijkt op dat van die terrorist. Deze methode wordt ook in de commerciële sector toegepast. Welk *type* mens vertoont bepaald gedrag? Om vervolgens op individueel niveau te kijken bij welk type iemand hoort. Surveillance als middel om mensen in categorieën te plaatsen.[71]

Als je de wereld door Lyons bril bekijkt, zie je social sorting overal. Al moet je soms goed kijken, want het sorteren gebeurt vaak buiten ons blikveld, in de databanken van grote bedrijven en organisaties, met verschillende technieken uit de computerwetenschappen. Zoals:

- *Datamining*, het doorzoeken van grote hoeveelheden data naar patronen. De Belastingdienst ziet in zijn data bijvoorbeeld dat pas gescheiden mensen hun belastingaangifte te laat invullen.
- *Risicoscoring*, het berekenen van kansen op verlies, winst, criminaliteit, ongeluk of andere te kwantificeren zaken. Op basis van je afbetalingsgedrag kun je bijvoorbeeld een slechte kredietscore hebben. Een bank verwacht dan dat je niet of te laat je lening terugbetaalt.

- *Machine learning*, een techniek die lijkt op datamining, maar bij machine learning gaat *de computer zelf* op zoek naar patronen, al dan niet begeleid door een mens. Na miljoenen simulaties vindt de computer dan bijvoorbeeld een correlatie tussen mannen die Britney Spears liken op Facebook en homoseksueel blijken te zijn. Er is niemand die dit de computer expliciet heeft verteld.
- *Profiling* is het doel dat je wilt bereiken en datamining en machine learning het middel. Een profiel is een categorie.
- *Algoritmes*, meestal gewoon software die een bepaalde taak procedureel afhandelt. Een recept is een algoritme. Je gebruikt alle ingrediënten in de juiste hoeveelheden en in de juiste volgorde en daar komt een lekker gerecht uit.

Wat deze profileringstechnieken gemeen hebben, is dat er gegevens worden verzameld, bewerkt, waar nodig verrijkt met nog meer data en dat er een geautomatiseerde bewerking op plaatsvindt. Dit proces heeft een uitkomst – een getal, kans, profiel of beoordeling – die vervolgens wordt gebruikt om onderscheid te maken tussen mensen.

Hoe Erik Pas gescoord werd

Terug naar de Amerikaanse avonturen van Erik Pas. Waarom zijn wij daar zo in geïnteresseerd? Omdat zijn reis social sorting in de praktijk laat zien.

Eerst bellen we Pas om van hem te horen hoe zijn reis stap voor stap is verlopen. Vervolgens spitten we tientallen documenten door op zoek naar informatie over Pas' gedrags- en persoonsgegevens. Bij iedere stap in zijn reis kijken we naar welke data zijn opgevraagd, door wie dat gedaan is en wat er vervolgens mee gebeurt. In de tientallen *privacy impact assessments* van het Ameri-

kaanse ministerie van Binnenlandse Veiligheid is te vinden wat het doel is van bepaalde dataverzamelingen, op welke rechtsgrondslagen die berusten, met wie informatie wordt gedeeld, hoelang die data worden bewaard en nog veel meer. Taaie kost, maar door dit soort informatie kunnen we achterhalen welke douanedatabases er zijn opgetuigd, wie daar toegang tot hebben en hoelang die gegevens worden bewaard. Op papier dan. Het uitvlooien van de datastromen van één enkele reis van één individu, van Amsterdam naar Los Angeles, kost ons uiteindelijk drie weken.

Hoe dat kan? Tot halverwege de jaren negentig was een vlucht naar de Verenigde Staten nog vrij eenvoudig. Je toonde je paspoort aan de douanier, werd gecontroleerd en als dat in orde was, kon je naar je vliegtuig.

Sinds *nine eleven* is het toezicht enorm uitgebreid. Naast een strenge fysieke controle worden steeds meer data verzameld en gebruikt om goedwillende reizigers van de kwaadwillenden te onderscheiden. Aan de hand van jouw data wordt een beeld opgebouwd van wie je bent en wat je intenties zijn. Dat beeld gaat vervolgens door een aantal filters.

Een van die filters is bijzonder relevant voor de reis van Pas. Het gaat om de ATS-P-database, wat voor Automated Targeting System-Passengers staat.[72] Dit systeem is sinds de aanslagen op nine eleven stukje bij beetje uitgebouwd. Uit verschillende documenten blijkt dat het drie dingen doet als je naar Amerika reist.

Ten eerste wordt van iedere reiziger een dossier aangelegd. Dat dossier bevat je boekinggegevens. Dit zijn de gegevens die je invult als je je reis boekt en als je een visum aanvraagt of met een ESTA-formulier toestemming vraagt om naar Amerika te reizen. Er staat bijvoorbeeld informatie in over wie je bent, waar je woont, wat je doet, hoe je eruitziet en, indien bekend, vingerafdruk, etniciteit, werkgevers- en opleidingsinformatie, inkomensgegevens, militaire ervaring, burgerlijke staat en de antwoorden die je hebt gegeven op ondervragingen door veiligheidsfunctionarissen.

Ten tweede word je vergeleken met allerlei zwarte lijsten van Amerikaanse opsporings- en inlichtingendiensten. Een beruchte is de No-Fly List, een lijst met enkele tienduizenden namen van terrorismeverdachten. Het ATS-P maakt daarnaast gebruik van de Selectee List en de Expanded Selectee List. Dit zijn lijsten van personen waartegen een verdenking nog niet goed onderbouwd is. Als je op zo'n lijst staat, mag je meestal wel vliegen, maar word je extra gecontroleerd. Tot slot levert ook het Center for Disease Control een zwarte lijst aan met mensen die om gezondheidsredenen niet aan boord mogen.

Ten slotte maakt ATS-P een risicoprofiel van iedere reiziger. Voor het maken van zo'n profiel gebruikt ATS-P ongeveer dertig verschillende databases. Daaruit wordt informatie gehaald over onder andere:

- Al je eerdere reizen naar Amerika. Wanneer dat was, met wie je reisde, waar je het land binnenkwam.
- Je ESTA-aanvraag, dus of je ooit gearresteerd bent geweest, een ziekte hebt gehad, een psychiatrisch verleden hebt, waar je naartoe gaat, waar je verblijft, je creditcardgegevens en je IP-adres.
- Of je ooit extra bent gecontroleerd bij aankomst en welke indruk de grensbewaker toen van je had.
- Je biometrische gegevens (vingerafdrukken, gezichtsscan) die je in het verleden hebt afgegeven bij de Amerikaanse douane.
- Inlichtingen van een aantal veiligheidsdiensten, zoals de CIA, FBI en regionale politie.
- En commerciële bronnen, van datahandelaren en sociale media.

Hoe het risicoprofiel precies wordt opgesteld, is geheim. Bekend is dat analisten van het National Targeting Center, een soort inlichtingendienst, je hele reis kunnen volgen en 'tactische beslissingen [kunnen] nemen op alle punten van het reiscontinuüm.'

In 2012 werden ruim 50.000 Europeanen onderworpen aan dergelijke 'tactische beslissingen.'

En de mogelijkheden voor extra controles zijn legio. Op het moment dat ATS-P een risicoprofiel van je maakt, heb je enkel nog je reis geboekt. Als je naar Schiphol gaat, word je gecontroleerd door de Koninklijke Marechaussee. Als je je bij de gate meldt, kunnen Amerikaanse agenten van het Immigration Advisory Program je nog aan een verhoor onderwerpen en allerlei databases raadplegen. Op het moment dat je vliegtuig opstijgt, gaat je paspoortinformatie naar de Amerikaanse douane, zodat die opnieuw een risico-inschatting kan maken. Als je aankomt op het vliegveld word je beoordeeld door Behavioral Detection Officers, die slechte intenties proberen te ontdekken door naar het gedrag van reizigers te kijken. Uit verschillende rapporten van de Amerikaanse Rekenkamer blijkt dat op sommige Amerikaanse luchthavens sensoren actief zijn die lichaamstemperatuur en bewegingen meten om kwaadwillenden eruit te pikken. Als je die filters achter de rug hebt, de douanier hebt gesproken, pas dan krijg je je stempel in je paspoort: *Welcome to America.*

Bij Pas ging het al fout in het ATS-P-systeem. Het bleek dat zijn internetprovider, Vodafone, een serie IP-adressen had opgekocht uit Jordanië en een daarvan had toegewezen aan Pas. Op het moment van boeken was de administratie van de IP-adressen nog niet bijgewerkt, waardoor de Amerikanen dachten dat hij zijn reis vanuit Jordanië had geboekt. Blijkbaar is dat verdacht. Zeker als de persoon beweert nog nooit in Jordanië te zijn geweest.

Misschien nog wel vervelender is dat alle informatie in ATS-P ten minste vijftien jaar wordt bewaard en beschikbaar blijft voor meerdere Amerikaanse inlichtingendiensten, zo staat in diverse privacy impact assessments. Ook behoudt het Amerikaanse ministerie van Binnenlandse Veiligheid het recht die informatie met 'buitenlandse partners' te delen.

Als Pas dus weer naar Amerika vliegt, is er een grote kans dat ergens weer een alarmbel afgaat. Hetzelfde geldt voor de tienduizenden Europeanen met vergelijkbare ervaringen.

Niet alleen reizigers van en naar de Verenigde Staten krijgen onbewust met risicoprofilering te maken, ook reizigers binnen de Europese Unie worden in kaart gebracht. Al jaren probeert de Europese Commissie het grenstoezicht in de EU 'te moderniseren.'

Na de aanslagen in Madrid (2004) en Londen (2005) heeft de Commissie het zogenoemde Smart Borders Project opgestart – een poging tot meer datagestuurde grenscontrole. Er zijn nieuwe databases opgetuigd met daarin informatie over immigranten en verdachten van misdrijven. Zoals het Schengen Informatie Systeem, het Visum Informatie Systeem en de vingerafdrukdatabase Eurodac. De Europese politieorganisatie Europol heeft meer bevoegdheden gekregen. Luchtvaartmaatschappijen moeten meer informatie leveren over passagiers die aan boord zitten. En, na meer dan tien jaar soebatten met het Europees Parlement, werd na de aanslagen in Parijs (2015) en Brussel (2016) wetgeving aangenomen die de uitwisseling van Passenger Name Records mogelijk moet maken. Alle Europese landen gaan vanaf 2018 dergelijke boekingsinformatie verzamelen en uitwisselen, mogelijk ook voor internationaal trein- en bootverkeer en voor reizen tussen de lidstaten. Ook wordt dan alle reizigersinformatie in Europa, net als in de Verenigde Staten, gebruikt om risicoprofielen van passagiers te maken.

De vraag is of in Europa net zo'n geoliede socialsortingmachine kan ontstaan als in de Verenigde Staten. Er bestaan voor Europese nationale overheden nog weinig verplichtingen om data met andere EU-landen te delen. En de analyses van de aanslagen op Europese bodem tonen telkens weer aan dat de internationale samenwerking van politie- en veiligheidsdiensten tekortschiet.[73]

Wat wel duidelijk is, is dat je steeds meer van jezelf moet blootgeven. Sterker nog, nu al kun je op *extra* reisprivileges rekenen als je bereid bent met de billen bloot te gaan en je vertrouwen hebt in de smetteloosheid van je data. Veel landen hebben een visumprogramma – in Nederland bijvoorbeeld Privium – waarmee een bepaald type passagier sneller door de douane komt. Om hiervoor in

aanmerking te komen, moet je van tevoren uitgebreide vragenlijsten en documentatie verschaffen en wordt er een veiligheidsonderzoek naar je uitgevoerd. Als daaruit blijkt dat je een laag risico vormt, mag je voortaan sneller en met minder controles de grens over.

Wat ook duidelijk is: de essentieelste handeling in dit hele proces – de daadwerkelijke beoordeling van wat verdacht is en wat niet – blijft geheim. We hebben allemaal een score, maar weten niet hoe hoog of laag die is en ten opzichte van wat. Ook hebben we geen idee of die klopt of eventueel aanpassingen behoeft. En deze social sorting blijft niet beperkt tot het internationaal reisverkeer.

Welkom in de gescoorde samenleving

Volgens technologieonderzoekers Frank Pasquale en Danielle Citron leven we in een *gescoorde samenleving*.[74] Dat is een samenleving waarin burgers scores krijgen toegekend door overheden, instanties, bedrijven en werkgevers. Die scores zijn berekeningen op basis van heel veel data en bepalen of je een bepaald recht krijgt of van een bepaalde dienst gebruik mag maken en tegen welke prijs. Ook voorspellen ze of je in de toekomst bepaald gedrag gaat vertonen.

Deze toekenning gebeurt volgens de onderzoekers zonder dat je het doorhebt. Welke persoons- of gedragsgegevens gebruikt worden, hoe de scores worden berekend én waarvoor ze worden gebruikt, blijft in nevelen gehuld. De scores kunnen beschouwd worden als een kwantitatieve vertaling van Lyons social sorting.

Begin 2015 liet een artikel in *de Volkskrant* de extreemste vorm van een gescoorde samenleving zien.[75] China heeft in 2014 plannen voor het Sociaal Kredietsysteem geïntroduceerd waarbinnen iedere Chinees een score krijgt toegekend voor zijn gedrag. De score wordt door de overheid en bedrijven voor tal van toepassin

gen gebruikt. Wie slecht scoort, wordt uitgesloten van bepaalde banen, huisvesting of kredietverlening, aldus de plannen.

Verschillende data bepalen die score: iemands schulden, iemands uitingen op sociale media én de scores van de mensen met wie iemand contact heeft. Zo wordt bijgehouden wat iemand leest, maar ook of volwassen kinderen wel vaak genoeg hun ouders bezoeken. Als die klagen, kan dat de sociale score van zoon of dochter negatief beïnvloeden.

Die score wordt niet alleen gebruikt om burgers te straffen. De aankoop van luiers bijvoorbeeld kan de score weer opkrikken, omdat dat op verantwoordelijk gedrag kan wijzen. En alles wat wijst op ondersteuning van de 'socialistische kernwaarden' wordt uiteraard ook beloond.

De beoogde Chinese samenleving doet denken aan die uit *The Circle*, de dystopische roman van Dave Eggers uit 2013. De Amerikaanse auteur beschrijft daarin de opmerkelijke carrière van May Holland, een jonge vrouw die bij een hip webbedrijf aan de slag gaat, The Circle, dat overduidelijk gemodelleerd is naar Google en Facebook. Bij The Circle draait het om radicale transparantie: alles wat je doet, moet zichtbaar en meetbaar zijn. En al je activiteiten worden gevat in een score: of je sociaal bent, een leuke collega, of je je targets haalt, of je bij een potentiële partner past. Eggers schetst zo een bedrijf en samenleving waarin iedereen lijkt te bezwijken onder de continue druk om de scores op peil te houden.

Ons punt is: de plannen voor het Sociaal Kredietsysteem in China en de wereld van *The Circle* zijn niet meer dan een uitvergroting van wat wij in het vrije Westen al jaren aan het doen zijn. Alleen gaat het in onze gescoorde samenleving niet om het behoud van 'socialistische kernwaarden,' of om radicale transparantie, maar om het minimaliseren van allerlei risico's – van wanbetaling tot terroristische aanslagen.

Een paar voorbeelden van vaderlandse bodem:

- Bijna alle Nederlanders hebben een kredietscore bij een van de bedrijven waar Maaike Goslinga in hoofdstuk 3 onderzoek naar deed. Die score wordt berekend op basis van kredietverleden, faillissementen, data van de Kamer van Koophandel en, steeds vaker, je sociale media en buurtgegevens. Die score bepaalt of jij een lening kunt krijgen en tegen welke rente en of je een telefoonabonnement kunt afsluiten.
- De gemeente Apeldoorn wil met behulp van inkomensgegevens, schoolverzuimdata, leeftijdsopbouw, politieaangiftes en voorzieningen in een bepaalde buurt voorspellen welke jongeren crimineel worden en daarop interventies gaan ontwerpen.[76]
- In het Elektronisch Kind Dossier krijgen alle jonge gezinnen een risicoscore toegewezen. Aan de hand van een lange vragenlijst wordt bepaald welke risicofactoren een gezonde ontwikkeling van het kind kunnen bedreigen, zoals verwaarlozing, mishandeling of een ongezonde levensstijl. Als sprake is van een opeenstapeling van risicofactoren kan worden ingegrepen door jeugdzorg, maatschappelijk werk of andere hulpverleners.
- Met SyRI wil de overheid uitkerings- en belastingfraude voorkomen. Uit een grote bak gegevens – over onder meer zorgverzekering, schulden, huisvesting en pensioenen – berekent de software een risicoscore voor iedere burger. Zo weet SyRI dat laag watergebruik op fraude kan duiden en neemt dat mee in de score. 'Alle burgers worden onderworpen aan een integriteitstoets,' zei emeritus hoogleraar Staats- en Bestuursrecht Margriet Overkleeft-Verburg daarover tegen ons. 'In feite krijgt iedere burger een rapportcijfer.'
- Ook de Belastingdienst werkt met risicoprofielen en scores op basis van de enorme hoeveelheden data die

> hij in huis heeft, zagen we in het vorige hoofdstuk. Zo bepaalt de fiscus wat de kansen zijn dat belastingplichtigen hun belastingen betalen, om vervolgens aan de hand daarvan 'iedere belastingbetaler de behandeling te geven die hij verdient.'

De taal en de beweegredenen van het Chinese systeem mogen anders zijn dan het Nederlandse, de logica is dezelfde: de scores die wij krijgen, doen een voorspelling over ons toekomstige gedrag, zonder dat we dat doorhebben.

Let wel, er zitten in Nederland geen kwade Big Brotherbedoelingen achter deze scoretoewijzingen. Overheden maken onderscheid tussen burgers door hen te scoren om maatschappelijke problemen efficiënter te bestrijden. Douaniers moeten veiligheid bieden, maar als er lange wachtrijen ontstaan voor de balie, worden passagiers en vliegtuigmaatschappijen boos. Zorgverleners willen bijtijds weten of er kinderen in de problemen dreigen te raken, maar kunnen simpelweg niet alle gezinnen bezoeken.

Ook bedrijven maken gebruik van scores, waar zowel het bedrijf als de klant – in theorie – voordeel bij heeft. We krijgen advertenties, diensten en producten die – volgens de aanbieders – aansluiten op onze behoeften. LinkedIn, Spotify en Netflix kunnen allerlei scores berekenen om je goede aanbevelingen te doen waardoor je net die juiste persoon bevriendt, dat prachtige liedje vindt of die bijzondere film ontdekt die je anders over het hoofd zou hebben gezien.

Dit zijn de evidente voordelen van het met scores onderscheid maken tussen burgers of consumenten. De nadelen zijn minder goed zichtbaar, maar als je beter kijkt minstens zo groot.

Foute data leiden tot foute beslissingen

Erik Pas' reis liet al een belangrijk nadeel van de geautomatiseerde scoring zien: foute data leiden tot foute beslissingen die amper te corrigeren zijn. Dat het nog erger kan, laat een aantal andere schrijnende gevallen van social sorting zien.

Neem Rahinah Ibrahim. Deze Maleisische vrouw woonde tientallen jaren in de Verenigde Staten en werkte daar aan een universiteit. In 2005 keerde ze voor korte tijd terug naar Maleisië. Toen ze weer naar Amerika wilde vliegen – naar huis dus – werd haar de toegang tot het vliegtuig ontzegd. Ook haar dochter, die de Amerikaanse nationaliteit heeft, mocht niet aan boord. De twee vermoedden dat ze op de No-Fly List waren terechtgekomen, maar de Amerikaanse autoriteiten wilden daar geen uitspraak over doen en weigerden hun toegang.

Na jaren juridisch getouwtrek kreeg ze haar zaak eindelijk voor een rechter. Zelfs tijdens de zitting wilde het ministerie van Binnenlandse Veiligheid niet zeggen of ze op de No-Fly List stond. Later bleek dat de FBI haar ten onrechte als terreurverdachte had aangemerkt. Dit vinkje werd verwijderd, maar loste het probleem nog niet op. De Amerikaanse ambassade in Kuala Lumpur weigerde niet veel later Ibrahim een visum te verstrekken. De reden? Onduidelijk. Haar dochter mocht wel terugreizen.

De zaak van Ibrahim is lang niet de enige. Hoeveel mensen de toegang tot vliegtuigen van en naar de Verenigde Staten wordt ontzegd, is niet bekend. Ook de selectiefilters waarin deze mensen blijkbaar blijven steken, zijn niet bekend.

Wel is duidelijk dat de No-Fly List blijft groeien. *The Intercept* legde in 2014 de hand op een handleiding voor het plaatsen van personen op de lijst.[77] 'Zonder enig bewijs kunnen mensen nu als terrorist worden aangewezen,' schreef het online medium. 'Ook machtigen de nieuwe richtlijnen één enkele functionaris van het Witte Huis om hele 'categorieën' mensen die door de overheid in de gaten worden gehouden op de No-Fly List [...] te zetten.'

Onderzoek op onderzoek wijst verder uit dat de lijst wemelt van de fouten. Geregeld mogen passagiers niet vliegen omdat ze toevallig dezelfde achternaam hebben als iemand op de lijst. Er staan zelfs overledenen op de No-Fly List. De voorbeelden van Erik Pas en Rahinah Ibrahim kun je afdoen als stomme pech. Je kunt ze ook zien als signaal van een dieperliggend probleem. Dit brengt ons bij de eerste fundamentele waarde die door grootschalig datagebruik in gevaar komt: ons burgerschap.

Ons burgerschap is in gevaar

Burgerschap is 'het recht om rechten te hebben.' Deze ware uitspraak deed politiek filosofe Hannah Arendt al in de jaren vijftig. Internationale mensenrechten zijn leuk en aardig, maar uiteindelijk moet de staat waarvan je burger bent ervoor instaan dat je van die rechten gebruik kunt maken.

John Cheney-Lippold haalt deze definitie vaak aan in zijn artikelen en lezingen.[78] Deze Amerikaanse mediaprofessor doet al jaren onderzoek naar burgerschap in tijden van Big Data, profiling en algoritmes. Volgens hem zijn veel overheden en bedrijven bevangen door dataïsme, een overdreven geloof in de mogelijkheden van data om onze werkelijkheid te beschrijven en vorm te geven. Meer data leiden volgens de gelovers altijd tot 'meer waarheid.'

Cheney-Lippold stelt dat het dataïsme als gevolg heeft dat het een nieuw soort burgerschap creëert, namelijk *voorwaardelijk* burgerschap.

Als voorbeeld noemt hij de NSA. De missie van die dienst kun je samenvatten met de slogan *'collect it all,'* die de dienst ook zelf hanteert in uitgelekte presentaties. Toch mag de NSA officieel alleen buitenlanders zonder moeite bespioneren. Het Amerikaanse ministerie van Justitie heeft in 2008 namelijk een 'minimalisatieprocedure' geformuleerd die moet voorkomen dat Amerikaanse staatsburgers door de NSA worden afgeluisterd. Opvallend genoeg

stelt diezelfde procedure dat als de kans dat iemand buitenlands is 51 procent is, die persoon wel bespioneerd mag worden. Of als iemand in de contactlijst staat van iemand die vermoedelijk 51 procent kans heeft om buitenlands te zijn. Of als iemand geen Engels spreekt. Of als iemand een IP-adres gebruikt dat zich buiten de Verenigde Staten bevindt.

Dit soort redeneringen leiden tot een vreemd soort burgerschap, betoogt Cheney-Lippold. Van oudsher kent dat twee vormen: jus sanguinis (burgerschap door bloed, van je ouders) en jus soli (burgerschap door bodem, waar je geboren bent). Volgens Cheney-Lippold is nu een derde vorm ontstaan: jus algoritmi (algoritmisch burgerschap). In tegenstelling tot jus sanguinis en jus soli geen vaststaand, maar een dynamisch burgerschap. Of je aanspraak kunt maken op het 'recht om rechten te hebben' hangt af van hoe je data op dat moment gewogen worden door een algoritme. Het ene moment kun je als Amerikaan, het volgende als buitenlander worden beschouwd. Maak je toevallig gebruik van een afwijkend IP-adres? Dan is er iets aan de hand, zoals Erik Pas merkte, en heb je opeens minder burgerrechten.

Schuldig tot het tegendeel bewezen is

Een van de rechten die burgers in gezonde democratieën beschermen, is de zogenoemde onschuldpresumptie: wij zijn onschuldig totdat het tegendeel bewezen is.

We spreken erover met hoogleraar ICT en Rechtsstaat Mireille Hildebrandt, een prominente stem in het Europees debat over privacy en surveillance. Zij beschrijft in haar in 2015 verschenen boek *Smart Technologies and the End(s) of Law* hoe de informatiesamenleving overgaat in een datagedreven maatschappij waarin technologieën gevoed door data onze levens sturen en voorspellen. Met als gevolg dat een aantal van onze fundamentele rechten – waaronder de onschuldpresumptie – onder druk komt te staan.

De onschuldpresumptie is op het eerste oog een tegenstrijdig recht. Want de presumptie gaat pas gelden als iemand ergens van verdacht wordt. 'Je wordt pas voor onschuldig gehouden als er vermoed wordt dat je schuldig bent,' zegt Hildebrandt.

Als er een concrete aanwijzing is dat jij iets crimineels gedaan hebt, krijg je recht op de rechten die horen bij de onschuldpresumptie, waaronder het recht te zwijgen en het recht te weten waarvan je verdacht wordt. Hildebrandt: 'Je bent eigenlijk extra beschermd als je verdacht bent.'

In het geval van predictive policing, het voorspellende politiewerk waar we in het vorige hoofdstuk over schreven, is dat anders. Die aanpak is volgens Hildebrandt onderdeel van de ontwikkeling dat opsporingsdiensten in toenemende mate 'preventief profileren.' Met datatechnologieën worden bepaalde categorieën mensen preventief als potentiële verdachten aangemerkt. Daarna *targeten* de diensten deze mensen: ze verzamelen meer data over hen, proberen ze meer te monitoren en meer te volgen. En daar wringt de schoen.

De burgers worden als een mogelijk verdachte behandeld maar kunnen geen gebruik maken van hun rechten. Dus: de diensten zullen graven in het leven van de als risico aangemerkte burgers, terwijl die burgers daar geen weet van hebben.

Toegegeven, zegt Hildebrandt, in de strikte zin van het woord blijft de onschuldpresumptie overeind in een datagedreven maatschappij. Want burgers worden niet aangeklaagd of veroordeeld zonder dat er bewijzen zijn aangeleverd en een rechter een uitspraak heeft gedaan. Aan de letter van de wet wordt ook in tijden van preventief profileren voldaan. Maar niet aan de geest van die wet, zegt Hildebrandt. 'Het *targeten* van mensen gebaseerd op geautomatiseerde beslissingen negeert het fundament van de onschuldpresumptie. Op die manier zijn alle burgers potentiële verdachten.'

Ook computers discrimineren

Een ander democratisch fundament is dat burgers in gelijke gevallen altijd gelijk behandeld moeten worden. Wat is zo'n belofte waard als je door een onzichtbare computerberekening in een vakje gestopt wordt dat leidt tot een andere behandeling? Of als je in een nieuwe categorie wordt gestopt die nog niet wettelijk beschermd is, zoals 'toekomstig crimineel'?

In mei 2016 legde geweldig onderzoek van de Amerikaanse journalistieke site *ProPublica* hiervan een pijnlijk voorbeeld bloot. In Amerika gebruiken steeds meer rechters programma's om de kans te berekenen dat een verdachte weer de fout in gaat.[79] Aan de hand van die berekening maakt de rechter een inschatting welke strafmaat gepast is. Heeft iemand een grote kans op recidive, dan moet-ie langer de gevangenis in. Zo moet het probleem van de overvolle gevangenissen bestreden worden.

Er zijn verschillende systemen in omloop die rechters kunnen gebruiken. *ProPublica* onderzocht de meest gebruikte scoringssoftware, die van het bedrijf Northpointe. Het programma gebruikt een vragenlijst die de verdachten zelf invullen of waarvan de antwoorden uit hun strafblad worden gehaald. Enkele vragen zijn:

- Heeft een van je ouders ooit in de gevangenis gezeten?
- Hoe vaak heb je op school gevochten?
- Heb je een baan?
- Hoeveel van je vrienden en kennissen gebruiken drugs?
- Word je snel boos?

Vervolgens krijgt iedere verdachte een score toegekend die de rechter gebruikt bij de bepaling van de strafmaat.

ProPublica neemt de proef op de som en vraagt van duizenden veroordeelden de scores en strafbladen op, die in de Verenigde Staten openbaar zijn. De bevindingen zijn niet mals.

Allereerst is de voorspellende waarde van het scoringssysteem

zeer gering. Van de groep veroordeelden die volgens het systeem grote kans hebben om weer geweld te gaan plegen, blijkt maar 20 procent dat ook echt te doen. 'Als we kijken naar een verzameling van verschillende misdrijven – waaronder kleine vergrijpen zoals rijden met een verlopen rijbewijs – dan is het algoritme iets accurater dan het gooien van kop of munt,' aldus *ProPublica*.

Ernstiger is dat het systeem discrimineert: het merkt zwarte Amerikanen vaker ten onrechte als potentiële recidivisten aan dan witte. Tegelijkertijd krijgen witte Amerikanen vaker ten onrechte een lage risicoscore dan zwarte. Naar ras wordt niet gevraagd in de vragenlijst, maar de opgetelde data werken toch in het nadeel van minderheden. De kans dat een ouder van een afro-Amerikaan heeft vastgezeten is bijvoorbeeld groter dan bij een witte Amerikaan. Deze statistische onevenwichtigheid werkt door in het puntensysteem van Northpointe.

Dat bedrijf weerspreekt overigens de bevindingen van *ProPublica* en weigert inzage te geven in de rekenmethodiek. De reden: 'bedrijfsgeheim.'

Het Amerikaanse datajournalistieke platform *FiveThirtyEight* wees in 2015 al op het risico op discriminatie met dergelijke geautomatiseerde systemen.[80] De data zelf gaan misschien niet over ras of sociale klassen, maar de kans dat je als zwarte in Amerika gearresteerd wordt voor drugsbezit, is wel groter dan wanneer je wit bent. Tegelijkertijd is het gebruik van drugs gelijk verdeeld over de bevolkingsgroepen. Die scheve verhouding komt ook weer terug in de risicoscore, omdat eerder drugsgebruik en eerdere veroordelingen als risicofactoren worden gezien.

De relatie tussen geautomatiseerde besluitvorming en discriminatie is de laatste jaren onderwerp van nieuw onderzoek. Op een privacyconferentie in Brussel horen we de jonge jurist Solon Barocas erover spreken en we zijn direct onder de indruk. Barocas heeft iets wat veel andere juristen, sociologen en filosofen niet

hebben: ervaring met technologie. Tijdens zijn studie internationale betrekkingen deed hij een extra opleiding tot data-analist. Inmiddels doet hij aan Princeton onderzoek naar geautomatiseerde besluitvorming.

In een artikel met jurist Andrew Selbst uit 2014 prikt Barocas een veelgehoorde belofte door, gedaan door belastingdiensten, veiligheidsdiensten en de Googles en Facebooks van deze wereld: dat de geautomatiseerde analyse van Big Data zou leiden tot rationele en daarmee eerlijker beslissingen.[81] Barocas en Selbst betogen dat de manieren waarop computers grote datasets verwerken, bestaande ongelijkheden in de samenleving juist vergroten en gereageld tot onbedoelde discriminatie leiden.

Barocas vertelt ons dat hij zich voornamelijk op machine learning richt. Dat speelt een steeds grotere rol in ons leven. Barocas geeft het voorbeeld van een bedrijf dat telefoondata gebruikt om de kans op terugbetaling van een lening te berekenen. 'Zij hebben een dataset van de belgeschiedenis van tienduizend telefoonabonnees én ze hebben een dataset met het kredietverleden van die mensen. Die voegen ze samen, waarop ze de computer vragen: als je nu kijkt naar hoe telefoons worden gebruikt, wat valt je dan op bij de mensen die hun schulden niet afbetalen? De computer zoekt en vindt patronen en komt met een antwoord. Bijvoorbeeld: 'Deze kandidaat kun je een lening verstrekken. De meeste mensen die hun telefoon op dezelfde manier als hij gebruiken, hebben in het verleden hun lening netjes terugbetaald.'

De computer gaat niet op zoek naar oorzaken voor dit verband. Hij ziet niet waarom die mensen hun lening terugbetalen. Hij ziet alleen dat dit bij het gevonden gedrag vaak gebeurt. Met andere woorden: met machine learning vind je alleen correlaties.

Volgens sommige techno-optimisten is zo'n correlatie genoeg. Al in 2008 schreef de Amerikaanse auteur Chris Anderson een invloedrijk essay met de veelzeggende titel *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*.[82] Wat is belang-

rijker, zo vroeg Anderson zich af: weten *dat* iets op een bepaalde manier werkt, of weten *waarom* iets werkt?

Google, zo stelt Anderson, hoeft geen talen te leren om een vertaaldienst aan te bieden. Het bedrijf heeft genoeg aan heel veel dezelfde woorden in verschillende talen en kan vervolgens de statistiek haar werk laten doen. Geef Google een woordenboek in Farsi en een woordenboek in Klingon, de taal van een volk in de televisieserie *Star Trek*, en het bedrijf vertaalt wel eventjes een intergalactisch gesprek.

'Dit is een wereld waarin enorme hoeveelheden data en toegepaste wiskunde iedere andere methode kunnen vervangen. Weg met al die theorieën over menselijk gedrag, van linguïstiek tot sociologie. Vergeet taxonomie, ontologie en psychologie. Wie begrijpt echt waarom mensen doen wat ze doen? Het punt is dát ze het doen, dat we dat kunnen volgen en meten met een ongekende betrouwbaarheid. Met genoeg data spreken de cijfers voor zichzelf,' schrijft Anderson.

Hij heeft een punt als hij zegt dat de immense hoeveelheden data heel veel nieuwe inzichten opleveren. Dat betekent niet dat als we blind op deze correlaties vertrouwen, zij onbevooroordeeld de waarheid vertellen.

Zo denkt Barocas er in ieder geval over. Het is een misvatting, zegt hij, dat computers neutraal hun berekeningen uitvoeren en dat de uitkomst daarvan dus objectief is. Het probleem van subjectiviteit los je niet op met machine learning. Sterker nog, machine learning kan die vooroordelen (onzichtbaar) versterken, wat tot toenemende discriminatie en maatschappelijke tegenstellingen kan leiden.

Want wie besluit wat je meet? Dat is en blijft een subjectief proces waarin ethische vragen bepalend zijn. Bijvoorbeeld: Wanneer is iemand een potentiële crimineel of terrorist? Hoe definieer je een onveilig gezin? En wie bepaalt wat een probleemleerling is?

Of neem kredietwaardigheid. Die wordt bepaald door te kijken naar iemands aflossingsverleden: heeft iemand een betalingstermijn gemist? Sommige beoordelaars kijken ook naar de samenstelling van iemands vriendengroep op sociale media: wordt iemand omringd door smoezelige zuiplappen of keurige veelverdieners? Het behoeft weinig verbeeldingskracht om te beseffen dat dit vooral voor achtergestelde bevolkingsgroepen nadelig kan uitpakken.

Daarnaast moet een kredietverstrekker over betrouwbare datasets beschikken. Dat is lastiger dan je denkt, vertelt Barocas, want veel data zijn vervuild.

In het vorige hoofdstuk zagen we al dat politiediensten misdaadstatistieken gebruiken om te bepalen waar ze gaan surveilleren of preventief fouilleren. Dat doen ze doorgaans in onveilige wijken waar veel minderheden wonen. Omdat de politie daar surveilleert, kan ze niet daar zijn waar misschien ook misdrijven worden gepleegd. Op die manier raken de statistieken vervuild, althans, vormen ze geen goede afspiegeling van wat er echt gaande is in de stad. En raken minderheden, die vooral in die slechte wijken wonen, oververtegenwoordigd in de misdaadcijfers.

Er zijn wijken in New York waar haast iedere bewoner minstens een keer per jaar preventief gefouilleerd wordt, simpelweg omdat de data aangeven dat er in die wijk veel aan de hand zal zijn. Noem het een selffulfilling prophecy.

Natuurlijk proberen dataminende overheden en bedrijven gevoelige informatie – data over geaardheid en religie bijvoorbeeld – uit hun analyses te houden, maar volgens Barocas is dat onmogelijk. Hij stelt dat veel op het oog onschuldige data toch gevoelige informatie kunnen onthullen. Je mag niet discrimineren op geaardheid bijvoorbeeld, maar iemand hoeft niet expliciet te zeggen dat hij homoseksueel is om daar door data-analyse toch achter te komen. In het vorige hoofdstuk beschreven we al wat het likegedrag van een Facebookgebruiker allemaal over die gebruiker bloot kan leggen, simpelweg omdat er bij een heel grote hoeveel-

heid mensen een verband bestaat tussen wat je liket en je seksuele geaardheid.

Die onvermoede verbanden zijn heel geniepig, meent Barocas. Zoals we in het vorige hoofdstuk al zagen: wat jij als onbelangrijke informatie ziet, kan voor een computer een duidelijke aanwijzing zijn over je seksuele geaardheid, gezondheid of andere gevoelige informatie. We krijgen daarmee een wereld waarin je geen stap meer kunt zetten zonder dat je heel veel van jezelf verraadt. Eenzelfde wereld waarin onderscheid wordt gemaakt tussen mensen op basis van data-analyse en waarin zo onbedoeld kan worden gediscrimineerd.

De solidariteit wordt ondermijnd

Een andere waarde die door grootschalige data-analyse en het scoren van groepen en individuen kan worden ondermijnd, is solidariteit. Dit laat zich het beste illustreren door het verzekeringswezen, dat steeds meer inzet op voorspellen op basis van data.

Het idee van verzekeren is dat het risico van individuele schade over een grotere groep mensen verspreid wordt. Als de één schade lijdt, kunnen de anderen dat opvangen. Wat gebeurt er nu: verzekeraars proberen die individuele risico's steeds meer op de schouders van die individuen te leggen. Enkele autoverzekeraars willen bijvoorbeeld je rijgedrag monitoren. Als je netjes rijdt, krijg je korting op je premie. Als je een slechte bestuurder bent, moet je misschien meer betalen.

Bepaalde zorgverzekeraars proberen inzicht te krijgen in het leefgedrag van hun klanten en willen zo gezond gedrag gaan belonen met een lagere premie en ongezond gedrag juist straffen door de prijs van de premie te verhogen. Intuïtief kun je dan denken: als we er betere chauffeurs en gezondere mensen van worden, waarom niet? Omdat deze ontwikkeling, zo beschreef hoofdredacteur Rob Wijnberg op *De Correspondent*, de solidariteit bedreigt.[83]

Hij schreef: 'Solidariteit is een manier om kosten en risico's gelijkmatig over een groep te verdelen. Dat gelijkmatige is daarin cruciaal: de kerngezonde jongere betaalt ongeveer evenveel zorgpremie als de zwakkere oudere uit solidariteit: zo blijft de zorg even betaalbaar voor hen die meer risico's lopen en kosten maken als voor hen die minder zorg nodig hebben. Verdisconteert de verzekeraar de risico's in de premie, dan ondergraaft hij daarmee precies dit principe van solidariteit.'

Als deze ontwikkeling doorzet – en wie naar de verzekeraars zelf luistert, weet dat dit zal gebeuren – dan bestaat het gevaar dat een systeem dat gebouwd is op het principe van solidariteit verandert in een systeem dat exact op het tegenovergestelde draait. Ga maar na: als de meeste mensen besluiten hierin mee te gaan, dan wordt het aanleveren van gezondheidsdata de norm. Dan is het verdacht om geen Fitbit om je arm te doen en is de kans groot dat verzekerden die de Fitbit weigeren, meer premie moeten betalen.

En het afstaan van onze data kan op nog een manier normerend werken, omdat de gemiddelde data die de analisten tot hun beschikking hebben de norm wordt. Om bij het voorbeeld te blijven: kleine kans dat een obese diabetespatiënt rond gaat lopen met een app die zijn suikerspiegel en transpiratieniveau meet en dit direct naar de verzekeraar doorsluist. Nee, er zullen hoogstwaarschijnlijk vooral gezonde mensen mee willen doen met dit soort metingen. Het datagedrag van de één – de gezonde jogger die voor premiekorting een Fitbit ombindt – heeft zo effect op het leven van de ander – de obese diabetespatiënt die meer premie moet gaan betalen.

Dit raakt aan een van de fundamentele principes achter profiling in het algemeen. Profielen worden opgesteld door analyse van de persoonlijke data van anderen. Denk aan Erik Pas. Hij was verdacht omdat zijn data aan een patroon voldeden dat andere verdachten hadden achtergelaten.

Het dataspoor dat wij – meestal onbewust – achterlaten, wordt gebruikt om anderen te sorteren en te targeten.

In zijn essay geeft Wijnberg niet alleen een moreel argument tegen scoren op basis van grote hoeveelheden data. Hij ziet het verdwijnen van solidariteit ook als een bedreiging voor de vooruitgang, doordat er 'een beloning komt te staan op risicomijdend gedrag.' Want: 'De ondernemer die achttien uur per dag werkt om zijn bedrijf tot een succes te maken, de journalist die gevaarlijke reizen onderneemt om oorlogen te verslaan, de sporter die de grenzen van het menselijke lichaam opzoekt: allemaal mensen die volgens de modellen van de verzekeraar meer kans maken op burn-outs, ongelukken of blessures. Maar ook stuk voor stuk mensen die een samenleving kleur geven en in de vaart der volkeren opstuwen. Juist omdat het kosten, risico's en lasten evenredig verdeelt, stelt het solidariteitsprincipe sommigen van ons in staat meer risico's te nemen en avontuur aan te gaan dan de doorsnee medemens. Gechargeerd gezegd: had Columbus een app in zijn broekzak gehad die zijn verzekeringspremie zou hebben aangepast aan zijn 'risicoprofiel,' dan was hij nooit uitgevaren om De Nieuwe Wereld te ontdekken.'

We verliezen onze autonomie

Tot nu toe gaat het over anderen die keuzes voor of over ons nemen. Douanesystemen die bepalen of wij mogen vliegen. Overheidsinstanties die berekenen of wij een risico vormen en ons navenant behandelen. Verzekeraars die ons een prijs rekenen aan de hand van wat zij als veilig of gezond gedrag beschouwen.

Maar hoe staat het met de keuzes die wij zelf maken? Hoe onafhankelijk maken we die? Laten we het eens hebben over een subtielere maar daarmee niet minder indringende vorm van beinvloeding. Hoe bepaalt de analyse van onze data welke informatie wij te zien krijgen en hoe beïnvloedt die voorgeselecteerde informatie ons gedrag?

Dagelijks komt er een onoverzichtelijke brij informatie op ons af. Als het goed is, sluit die aan op onze behoeften. Algoritmes kunnen inschatten welke informatie ons bevalt. Grote nieuwssites schotelen ons berichten voor die we willen lezen. Spotify doet suggesties voor nieuwe muziek. LinkedIn wijst ons op een interessante vacature die we anders over het hoofd hadden gezien.

Vaak hebben we niet door dat deze informatie geselecteerd is. Lang dachten we dat alle Facebookberichten van onze vrienden chronologisch getoond worden. Niets is minder waar: we krijgen slechts een fractie voorgeschoteld, die het resultaat is van een aantal geheime algoritmische beslissingen. En lang dachten wij via Google een volledig neutrale weergave van alle mogelijke zoekresultaten te krijgen, maar ook 's werelds populairste zoekmachine is een sorteermachine in vermomming: de resultaten zijn gepersonaliseerd en datagestuurd. De ene persoon die naar 'Egypte' zoekt, krijgt allerlei vakantiesites te zien, de andere worden vooral nieuwssites voorgeschoteld. En ook bij Google is het recept dat de volgorde bepaalt zo geheim als dat van Coca-Cola.

Moeten we deze nieuwe technologie vrezen? Nee, zeggen informatici Maarten de Rijke en David Graus van de Universiteit van Amsterdam. In juni 2016 publiceerden zij een inzichtelijk opiniestuk in *nrc.next* over de aanzwellende kritiek op het gebrek aan neutraliteit van het sociale medium en de zoekmachine.[84]

Volgens De Rijke en Graus is dat gebrek aan neutraliteit juist wenselijk. 'Het is wat de zoek- en aanbevelingssystemen in staat stelt ons toegang te geven tot de bergen informatie, en ons nieuwe muziek of films te laten ontdekken,' schreven de informatici. 'Met objectieve, neutrale, algoritmen zouden we niets meer kunnen vinden.'

Of informatie nuttig is, verschilt immers per persoon en er is zoveel informatie dat er grondig gefilterd moet worden. 'In de context van, bijvoorbeeld, Facebooks newsfeed, Googles zoekresultaten of aanbevelingen van Netflix wordt een machine niet ver-

teld wat te doen, maar verteld om te leren wat te doen. De systemen leren van subjectieve bronnen: onszelf, onze voorkeuren, ons interactiegedrag. Het leren van subjectieve bronnen zorgt vanzelfsprekend voor subjectieve uitkomsten.'

We moeten dit soort zoek- en aanbevelingssystemen daarom vooral zien als een informatietussenpersoon, zeggen De Rijke en Graus. 'Net als traditionele informatietussenpersonen (journalisten, artsen, opiniemakers) geeft [het systeem] een standpunt weer door informatie te filteren en te rangschikken. En net als bij traditionele tussenpersonen doet men er verstandig aan om een tweede of derde mening te vragen als het er werkelijk toe doet.'

Moeten we dergelijke technologieën dus omarmen? We gaan te rade bij de Twentse technologiefilosoof Peter-Paul Verbeek. Een optimist die zich verzet tegen doemdenkerij over nieuwe technologieën. 'De eerste brillen werden ook met veel argwaan bekeken,' vertelt hij. 'Je deed een ingreep in de menselijke natuur en dat is altijd omstreden. Vóór de bril konden sommige mensen zien en anderen niet. Heel simpel. Opeens werd dat maakbaar. We hadden het idee dat we op de stoel van God gingen zitten. De versmelting van mens en technologie heeft altijd iets overmoedigs, maar we hebben die bril toch echt een plek in ons bestaan gegeven.'

Verbeek neemt een middenpositie in binnen de techniekfilosofie. Anders dan veel andere denkers interesseert hij zich niet zozeer in de vraag óf we nieuwe technologie wel moeten toelaten. 'Het gaat niet over 'ja' of 'nee,' maar over 'hoe.' We moeten onszelf stileren in interactie met technologie.' Met andere woorden: we moeten leren omgaan met de invloed van de technologieën om ons heen.

De vraag is hoe je jezelf kunt 'stileren in interactie' met een algoritme waarvan je niet weet hoe het werkt of waarvan je het bestaan überhaupt niet kent. 'Het op ondoorzichtige wijze beïnvloeden van onze overtuigingen en gedragingen is wel echt een nieuwe stap,' beaamt Verbeek. 'Er wordt met deze algoritmen,

zonder dat mensen het doorhebben, beslist wat ze wel of niet belangrijk vinden. Er zit een soort vooringenomenheid in wat de machine jou teruggeeft. Er wordt je een venster op de wereld aangereikt.' Lachend: 'Google is eigenlijk al een bril, onze bril op de wereld, die bepaalt hoe we de wereld ervaren. Het is zaak dat we die ervaring goed in ogenschouw houden.'

Hoe doe je dat? Hoe zorg je ervoor dat je de invloed van Google door blijft hebben? Of van de Belastingdienst? Verbeek ziet hier een belangrijke rol weggelegd voor journalisten, filosofen en wetenschappers. 'Er moeten mensen zijn die gedetailleerd in kaart brengen wat de subtiele effecten van technologie op ons dagelijks leven zijn. De meeste mensen weten dat autoverkopers je proberen te verleiden en dat politici in campagnetijd er alles aan doen om je stem te winnen. Zoals wij omgaan met autoverkopers en politici, zo moeten wij ook omgaan met apps en software.'

Er is eigenlijk maar één grens, zegt Verbeek. 'Als je de invloed van het algoritme op geen enkele manier meer kunt doorzien, dan is er geen gelijkwaardige interactie meer mogelijk. Dan gaat de techniek met jou om in plaats van andersom.' En eerder zei hij al: 'Wat mij betreft is de verantwoordelijkheid voor het eigen bestaan een grens die nooit overschreden mag worden. Als je [...] de technologie niet meer van een afstand kunt bekijken, dan houd je op te bestaan. Dat is de enige echte grens van de mens.'

Dat zijn zware woorden, zeker voor een rasoptimist als Peter-Paul Verbeek. Toch is dit een angst die onder veel experts leeft: dat de menselijke autonomie onder druk komt te staan door het grootschalig gebruik van onze gegevens, zonder dat we ons daar bewust van zijn. Dit heeft evident individuele gevolgen, maar keuzevrijheid en autonomie zijn óók cruciale bouwstenen van een gezonde democratie.

Mister Orange en de beïnvloeding door bedrijven

Een illustratie van het verlies van autonomie door gebruik van persoonlijke data komt van de Israëlische rechtsgeleerde Tal Zarsky.[85] In Zarsky's fictieve voorbeeld wil een man – Mister Orange geheten – stoppen met roken. Bij de online winkel waar hij normaal sigaretten bestelt, koopt hij nu nicotinepleisters. Wat hij niet weet, is dat de online winkel dat registreert en hem nu op andere sites advertenties van zijn favoriete sigarettenmerk voorschotelt én hem een 'extra' pakje sigaretten aanbiedt bij de bezorging van zijn boodschappen.

Mister Orange weet niet dat iemand anders weet dat hij van plan is om te stoppen. Nee, het enige wat hij gedaan heeft is zich iets anders gedragen: hij heeft die week geen sigaretten gekocht én nicotinepleisters besteld. De online winkel heeft deze gedragingen tezamen opgemerkt en geïnterpreteerd en probeert Mister Orange van gedachten te doen veranderen door hem op bepaalde momenten bepaalde informatie voor te schotelen. Voor Mister Orange lijkt dit informatie die iedereen te zien krijgt. Hij heeft geen idee dat hij een target is van de winkelier die hem zijn lucratieve nicotine wil blijven verkopen.

Los van de vraag of deze strategie werkt, noemt Zarsky deze vorm van beïnvloeding een aanval op Mister Orange' autonomie, juist omdat Mister Orange het niet doorheeft. Om ons niet te verliezen in een eeuwenoud dispuut onder filosofen over de betekenis van 'autonomie,' hanteren we hier de alledaagse betekenis van het begrip: dat een autonoom persoon iemand is die in staat is zelf beslissingen te nemen. Het woord komt van het Griekse *autos* (zelf) en *nomos* (eigen wetten opleggend) en betekent dat een individu zichzelf wetten op kan leggen, vrij van inmenging door anderen.

Nu zou je kunnen tegenwerpen dat Mister Orange nog steeds zelf beslist of hij stopt of doorgaat met roken. Als hij besluit te blijven roken, dan is dat zijn eigen keuze en niet het resultaat van een gebrek aan autonomie, toch?

Niet helemaal. Autonomie is ook een reflexieve waarde. Dat wil zeggen dat een autonoom persoon in staat is kritisch te reflecteren op de keuzes die hij kan maken. Dat hij, bijvoorbeeld, zijn eigen wensen en voorkeuren kan beoordelen en daarnaar kan handelen. Als Mister Orange onbewust beïnvloed wordt door de advertenties of het pakje sigaretten in zijn boodschappentas en doorgaat met roken, is hier geen sprake van. Hij heeft de invloed simpelweg niet door, anders dan bij ouderwetse advertenties, die hij met eigen ogen kon zien.

'Subliminale manipulatie,' noemt Mireille Hildebrandt deze beïnvloeding. We worden een bepaalde kant opgeduwd, zonder dat we het doorhebben. In haar boek *Smart Technologies and the End(s) of Law* gaat de hoogleraar ICT en Rechtsstaat Hildebrandt in op het voorbeeld van supermarktketen Target, die aan de hand van data kon voorspellen wie van haar klanten zwanger was. Een artikel over Target in *The New York Times* kreeg in 2012 enorm veel aandacht.[86] Vooral de passage waarin beschreven werd hoe de vader van een meisje van achttien woedend contact opnam met Target en zei dat het bedrijf op moest houden zijn dochter al die aanbiedingen te doen; zij was helemaal niet zwanger. Later bood de man zijn excuses aan. Zijn dochter bleek wel degelijk zwanger, alleen wisten de data crunchers van Target dat eerder dan haar vader.

Dit verhaal deed het zo goed omdat het de kracht van datamining illustreerde en tegelijkertijd een wat creepy gevoel veroorzaakte bij de toehoorders.

Hildebrandt legt liever de nadruk op een ander deel van het artikel in *The New York Times*. In deze passage beschrijft een leidinggevende van Target dat sommige zwangere vrouwen ronduit negatief reageerden toen zij erachter kwamen dat het bedrijf zoiets intiems van hen wist zonder dat zij die informatie zelf hadden gegeven. Dus wat deed het bedrijf? Het begon de coupons en acties te vermengen met advertenties waarvan Target wist dat zwangere vrouwen de aangeprezen producten nooit zouden ko-

pen. 'Wij plaatsen een advertentie voor een grasmachine naast een advertentie voor luiers,' aldus de Targetvertegenwoordiger. 'Wij zetten een coupon voor wijnglazen naast die van kinderkleren. Op die manier leek het alsof de producten bij toeval waren gekozen.' En dat werkte. 'We kwamen erachter dat zolang een zwangere vrouw denkt dat ze niet bespioneerd wordt, zij de coupons gebruikt.'

Een perfecte illustratie van het verlies van autonomie. In het eerste geval besluit een deel van de vrouwen niet in te gaan op de verleidingspoging omdat de geboden keuze hun niet bevalt. In het tweede geval is er sprake van de 'subliminale manipulatie' waar Hildebrandt over spreekt. Dit is effectief – juist doordat de zwangere vrouw het niet doorheeft. In de woorden van de leidinggevende van Target: 'Zolang we haar niet bang maken, werkt het.'

Hildebrandt vergelijkt dit soort online manipulatie met A/B-testen, een gangbare manier voor sites en online diensten om veranderingen te testen op gebruikers. Op internet worden we continu aan dergelijke testen blootgesteld, zonder dat we het doorhebben.

Nieuwssites als *The New York Times* maken er ook gebruik van. Een groep mensen krijgt titel A boven een stuk te zien en een andere groep mensen titel B. Vervolgens wordt gemeten welke titel tot meer bezoekers leidt. Als een titel duidelijk beter werkt dan de andere, krijgen alle nieuwe bezoekers die te zien.

Als je wilt optimaliseren, kun je ook complete websites testen. Je toont bezoekers verschillende versies, waarbij kleine aanpassingen zijn doorgevoerd. Denk aan andere kleurstellingen, links, lettertypes of commerciële boodschappen. Vervolgens wordt het gedrag van de bezoekers gemeten. Op welke site blijven ze langer, klikken ze meer, geven ze meer geld uit, komen ze vaker terug? De versie waar de bezoekers het meest het gewenste gedrag vertonen, blijft. Vervolgens herhaalt dit proces zich, met versie C, et cetera. Zo zijn we op het internet continu onderdeel van een experiment. Hildebrandt: 'Ik ben niet per se tegen A/B-testen en

experimenten. Ik ben ertegen dat wij het met zijn allen niet doorhebben.'

En als we het ineens wél doorhebben, is de ophef groot. In augustus 2014 openbaarde de oprichter van de Amerikaanse datingsite OkCupid een aantal experimenten dat de site – zonder medeweten van zijn gebruikers – had uitgevoerd.[87] Zo werden op een dag alle profielfoto's verwijderd om te kijken wat het effect daarvan zou zijn. Voor een ander experiment verwijderde de site profielteksten om na te gaan hoe gebruikers met alleen een profielfoto in de smaak vielen. Voor een derde experiment meldde de datingsite sommige gebruikers dat zij een goede match hadden met iemand waarmee zij volgens de berekeningen van OkCupid juist een heel slechte klik hadden.

Het bericht waarin de oprichter deze experimenten opbiechtte, was licht laatdunkend van toon: 'Wat denk je dan! Als je het internet gebruikt, ben je altijd onderwerp van honderden experimenten. Zo werken websites nu eenmaal.' Hoe aanmatigend dit misschien ook klinkt, de oprichter van OkCupid had wel gelijk. Zo werkt het web.

Toen Facebook in diezelfde periode bekendmaakte dat het sociale medium in 2012 een groot psychologisch onderzoek onder bijna 700.000 gebruikers had uitgevoerd, waren de reacties ook niet mals.[88] Zonder dat de gebruikers er weet van hadden, manipuleerden de onderzoekers hun newsfeed zodat zij óf voornamelijk positieve óf voornamelijk negatieve berichten te zien kregen. Zo wilde Facebook onderzoeken of emotie 'besmettelijk' was en of, met andere woorden, gebruikers die vooral negatieve berichten te zien kregen, zelf ook meer negatieve berichten zouden plaatsen. En het werkte. Gebruikers gingen mee in de emotie van hun Facebookvrienden.

Beïnvloeding door overheden

Niet alleen commerciële partijen vormen een bedreiging voor de menselijke autonomie. Overheden en publieke instanties maken in toenemende mate ook gebruik van dergelijke beïnvloedingstechnieken – in het vorige hoofdstuk beschreven we al de nudge-ambities van de Belastingdienst. De cruciale vraag is: weten we dat we door de overheid genudged worden, of worden we onbewust beïnvloed om bepaald gedrag te vertonen?

De fiscus geeft toe dat hij nudgetechnieken toepast, onder andere bij gescheiden stellen. Hoe ontwikkelt de fiscus zich verder op dit vlak? En zijn andere overheidsdiensten ook de mogelijkheden van nudging aan het verkennen? Nogmaals: Big Data-nudging door overheden staat nog in de kinderschoenen (althans: voor zover wij weten!). Maar wie toekomstplannen van regeringen doorleest, met hoge ambtenaren spreekt of nadenkt over de evidente voordelen die dit type nudging kan hebben voor overheden met sociale beheersingsdrang, weet dat dit in de toekomst alleen maar meer zal gebeuren.

En dit is ook een honderd procent veilige voorspelling: de hoeveelheid en typen data die overheidsdiensten tot hun beschikking krijgen, zullen blijven toenemen. Waardoor overheden – eventueel in samenwerking met bedrijven – burgers steeds gerichter kunnen beïnvloeden. Het is niet ondenkbaar dat de druk van de waterleiding door een waterbedrijf hoog zal worden gehouden als de meeste gezinsleden douchen. Of dat de ijskast een bepaald geluid maakt als de inhoud van de ijskast al een paar dagen niet meer aan de Schijf van Vijf voldoet. Of dat de elektriciteit na tienen wordt uitgeschakeld om de kosten voor de bewoner met een uitkering te drukken.

Met meer data en geavanceerdere analysemethoden zullen er steeds meer correlaties gevonden worden tussen typen gedrag en typen mensen. Dit biedt de overheden de kans om burgers dynamisch en realtime te nudgen. De vraag is wanneer wij dergelijke nudges nog als zodanig kunnen onderscheiden. Wanneer een goedbedoeld duwtje in de rug overgaat in keiharde manipulatie. Tot welk punt wij in vrijheid kunnen kiezen en wanneer we geen keuze meer hebben.

Een van de belangrijkste rechten die burgers in een democratie hebben, is het recht hun eigen volksvertegenwoordigers te kiezen. Daarbij is het van belang dat burgers vrij van inmenging door anderen hun keuzes kunnen maken. Kiezen ze Donald Trump of Hillary Clinton? PVV of toch weer SP?

Volgens psycholoog Robert Epstein staat het ideaal van de burger die geheel autonoom zijn stem uitbrengt onder druk. En wel door Google. Jarenlang onderzocht Epstein de potentiële invloed van de zoekmachine op kiezers. Preciezer geformuleerd: het effect van de zoekresultaten op hun politieke voorkeur.

Zo voerde hij een interessant experiment uit in India, vlak voor de landelijke verkiezingen in 2014.[89] Epstein verdeelde zijn proefpersonen – ruim 2.000 kiesgerechtigde Indiërs die nog niet wisten op welke partij ze zouden stemmen – over drie verschillende groepen. Iedere proefpersoon kreeg de opdracht te googelen naar de lijsttrekkers van de drie grootste Indiase partijen.

De zoekresultaten die de proefpersonen te zien kregen, waren door Epstein gemanipuleerd. Bovenaan de lijst verschenen per groep uitgesproken positieve artikelen over één kandidaat, terwijl de positieve artikelen over de andere twee kandidaten juist onderaan de zoekresultaten waren geplaatst.

Na afloop vroeg Epstein zijn proefpersonen welke kandidaat hun voorkeur had. Ze bleken vaker geneigd voor de kandidaat te stemmen bij wie de positieve artikelen bovenaan hadden gestaan. Epstein beweert op basis daarvan dat hij in staat is het aantal stemmen voor een kandidaat gemiddeld met ruim 12 procent te verhogen.

Epstein beweert overigens niet dat Google daadwerkelijk verkiezingen manipuleert. De psycholoog stelt wél dat het bedrijf *de*

macht heeft om de voorkeuren van bepaalde stemgerechtigden te veranderen. Daarbij komt dat, mocht het bedrijf wél verkiezingen manipuleren, die beïnvloeding onmogelijk te bewijzen zou zijn: de resultatenpagina's van Google-zoekopdrachten worden niet opgeslagen.

Er is het een en ander aan te merken op Epsteins onderzoek. Zo heeft de psycholoog voortdurend de neiging om zijn onderzoeksresultaten uit te venten nog voordat het onderzoek gepubliceerd is. De onderzoeker schroomt ook niet om in populaire media in stevige bewoordingen de consequenties van zijn onderzoek te benadrukken. Daarnaast lijkt zijn werk nog weleens het karakter te hebben van een persoonlijke vete tegen Google, waar Epstein ooit een juridisch conflict mee had.

Het mag de vraag zijn hoe degelijk Epsteins onderzoek is, het raakt wel aan een gevoelig punt. We hebben de neiging om de voorgeschotelde informatie van platforms als Google of Facebook als neutraal te beschouwen. Maar achter die ogenschijnlijke neutraliteit schuilen platforms die subjectieve keuzes maken in hoe zij hun poortwachtersfunctie vormgeven, in wat ze ons wel en wat ze ons niet laten zien. Zij zijn onze bril op de samenleving. Zonder dat we weten hoe die bril gemaakt is, wat hij wel en niet toont en dat we hem überhaupt ophebben.

De democratische samenleving onder druk

We besluiten dit hoofdstuk met onze favoriete technologiedenker Evgeny Morozov. Op polemische toon bekritiseert Morozov al jaren het heilige geloof in digitale technologieën die de wereld moeten redden. Hij noemt het *solutionism,* het idee dat er voor ieder probleem – hoe complex en gelaagd ook – een technologische oplossing is.

Zijn ideeën over privacy sluiten naadloos aan op een van de

belangrijkste conclusies van onze zoektocht. Privacy is een voorwaarde voor andere waarden, legt Morozov ons uit in een statig grachtenpand in Amsterdam. 'Ik zie privacy als een manier om toegang te krijgen tot een veilige en private ruimte, waar je kunt reflecteren op de wereld, een mening kunt vormen, kunt bedenken hoe je het systeem anders wilt zien.'

Tot zover herhaalt Morozov een (van de vele) woordenboekdefinitie van privacy. Maar nu komt de crux: daar houdt het niet op, zegt Morozov. Die veilige private ruimte is nodig, aldus de denker, 'om vervolgens terug te keren naar het publieke forum en bij te dragen aan de verbetering van het systeem, jouw mening in te brengen en te debatteren.'

Met andere woorden: privacy is essentieel voor een gezond democratisch debat. En precies deze voorwaarde staat onder druk door nudgende overheden en surveillancekapitalisten, aldus de Wit-Russische denker.

Het échte privacyprobleem, vat hij het voor ons samen, is niet dat wij de controle kwijt zijn over onze persoonlijke data. Of dat overheden en bedrijven zo bizar veel over ons weten. Nee, het probleem is dat overheden en bedrijven al die data gebruiken om ons in bepaalde richtingen te duwen – zonder dat wij het doorhebben. 'Onzichtbaar prikkeldraad,' noemt hij het. De algoritmes en datagestuurde informatie van overheden en bedrijven bepalen onze keuzes, zoals prikkeldraad onze bewegingsvrijheid bepaalt. Dit prikkeldraad '[limiteert] onze levens tot een plek die er rustig en aantrekkelijk uitziet, maar die wij niet zelf hebben gekozen en die we niet kunnen herbouwen of uitbreiden. Het ergste van alles is dat wij het niet als zodanig zien, het prikkeldraad blíjft onzichtbaar.'

Dat is waar de discussies over privacy en data over zouden moeten gaan, stelt Morozov. Over het onzichtbare prikkeldraad dat de menselijke autonomie – en daarmee de democratie – in gevaar brengt. Sterker, het dominante gesprek over privacy – namelijk dat onze privacy gered is als iedereen maar controle heeft over zijn

eigen gegevens – kan zelfs gevaarlijk zijn, zegt Morozov. ‘Ik kan mij makkelijk een wereld voorstellen waarin iedereen totale controle over zijn data heeft, maar niemand meer iets bijdraagt aan de publieke sfeer.’

'Anderen grondig onderzoeken maar zelf grondig onderzoek door anderen vermijden, is een van de belangrijkste vormen van macht.'[90]

– HOOGLERAAR RECHT FRANK PASQUALE

'De geschiedenis toont dat als mensen zien hoe machtsmachinaties hun dagelijks leven beïnvloeden – mijn kredietwaardigheid, mijn banksaldo, mijn premies, mijn rechten en mijn vrijheid – zij sneller in opstand zullen komen. Onze onverschilligheid is een zegen voor hen.'[91]

– HOOGLERAAR BUSINESS ADMINISTRATION SHOSHANA ZUBOFF

Conclusie

Tijd voor tegenmacht

Aan de uitspraak 'ik heb niets te verbergen' ligt een aantal fundamentele aannames ten grondslag:

- De eerste aanname is dat degene die dit zegt, weet *wat* het is dat hij niet te verbergen heeft.
- De tweede is dat hij weet *voor wie* hij dat niet te verbergen heeft.
- De derde is dat hij weet *waarom* hij dat niet te verbergen heeft.

Uit de zoektocht in dit boek blijkt dat alle drie de aannames misvattingen zijn. Want we weten helemaal niet welke gegevens we allemaal weggeven. We hebben geen idee wie er – bevoegd of onbevoegd – toegang tot die data hebben. En we weten niet om welke redenen andere partijen in onze data geïnteresseerd zijn, wat ze ermee doen en welke beslissingen over ons worden genomen op basis van die data.

Hoe kun je dus zeggen dat je niets te verbergen hebt als je niet weet welke datasporen je achterlaat? Hoe kun je zeggen dat je niets te verbergen hebt als je niet weet wie er bij jouw data kunnen? Hoe kun je zeggen dat je niets te verbergen hebt als je niet weet wat er met jouw data gebeurt?

En dan is er ook nog de aanname van de 'ik' in de zin 'ik heb niets te verbergen.' Het woord dat privacy tot een persoonlijke in plaats

van een collectieve aangelegenheid degradeert, er een puur individuele in plaats van een collectieve waarde van maakt.

Laten we het dus gewoon benoemen: wie 'ik heb niets te verbergen' zegt, weet niet waar hij het over heeft.

De machtsongelijkheid

En we *kunnen* het ook helemaal niet weten. Constant lopen we tegen enorme informatie-asymmetrieën aan. Tussen ons en de technologieën om ons heen; tussen ons en de bedrijven wier producten en diensten we gebruiken en tussen ons en de overheden waar we als burgers afhankelijk van zijn. Wij doorgronden hen nauwelijks, terwijl zij ons tot in onze diepste vezels leren kennen.

De balans is volslagen zoek.

De Amerikaanse auteur Frank Pasquale noemt de huidige maatschappij een '*Black Box Society*.' Een samenleving waarin wij omringd zijn door steeds onbegrijpelijker en geheimzinniger wordende black boxes. Deze black boxes, stelt Pasquale, zijn zowel technologieën en apparaten als instituties en systemen wier werking voor ons verborgen blijft. 'Wij komen met beide dagelijks in aanraking,' schrijft Pasquale. 'Terwijl we steeds meer getrackt worden door bedrijven en de overheid, hebben we geen idee meer waar onze informatie allemaal belandt, hoe die gebruikt wordt en wat daar de consequenties van zijn.'

Dit begint al bij de constatering dat we geen idee hebben welke digitale sporen we achterlaten. De locatie van je smartphone. De apps die je installeert. De manier waarop je autorijdt. De sites die je bezoekt. Of je rookt of drinkt. Waar je met je creditcard betaalt. Wie jouw digitale vrienden zijn.

Je kunt er niet voor kiezen of je deze persoonlijke gegevens wel of niet wilt delen. Technologiebedrijven zijn ronduit vaag over wat ze van je weten en wat ze met je informatie doen. De algemene en de privacyvoorwaarden zijn zo opgesteld dat je ze vooral niet leest.

En lees je ze wel, dan kom je er vaak achter dat de enige keus die je hebt een binaire is: wel of niet gebruikmaken van een dienst.

Bovendien blijken de partijen die over onze data waken keer op keer ons vertrouwen te schaden. Bedrijven beveiligen onze data regelmatig ronduit slecht. Je kunt als gewone gebruiker niet beoordelen of een dienst of product wel veilig is. Intussen willen overheden óók toegang krijgen tot onze gegevens en dwingen ze bedrijven die te overhandigen. Zo bezien is het vreemd dat wij onze data aan derden blijven toevertrouwen. Aan de andere kant: hebben we wel een keuze?

En kom er maar eens achter wie er toegang tot je data heeft. De overheid is een informatiestromenland en weet zelf niet welke gegevens ze van burgers heeft en hoe die tussen verschillende instanties en overheidslagen worden uitgewisseld.

Tegelijkertijd is het onmogelijk om te ontkomen aan de lange armen van Google, Facebook en datahandelaren – ook als je nog nooit direct met deze bedrijven in contact hebt gestaan. Surveillance is het verdienmodel van het internet. En vindt, zoals alle succesvolle vormen van spionage, buiten je zicht om plaats.

Wat jij ook al niet ziet, is hoe bedrijven en overheden, die socioloog James Rule sociale beheersers noemt, over jou denken. Zij willen jou zo goed mogelijk leren kennen zodat ze je in een bepaalde richting kunnen duwen. De sociale beheersers – van de Belastingdienst tot Google – willen uiteindelijk jouw gedrag beïnvloeden – van het netjes op tijd belastingen betalen tot het klikken op een advertentie. Om je te kunnen sturen, brengen zij jou en jouw gedrag in kaart, proberen zij jouw drijfveren te achterhalen. En jij? Jij ziet het niet en kunt het beeld dat ze van je maken niet corrigeren.

Facebook bepaalt wat jij te zien krijgt van wat jouw vrienden doen. Google beslist welke informatie jij tot je kunt nemen. De bank huurt een onbekende partij in om te adviseren of jij geld mag lenen. De Belastingdienst calculeert of jij een toekomstige fraudeur bent. Ministeries rekenen uit of jij een risicoburger bent die bepaald ongewenst gedrag kan vertonen.

Dat is macht: onder de deksels van al die zwarte dozen worden er beslissingen over en voor ons genomen. In de woorden van Helen Nissenbaum en haar collega Finn Brunton: 'Diegenen die ons kennen, hebben macht over ons. Zij kunnen ons een baan ontzeggen, een lening onthouden, onze bewegingen inperken, ons onderdak, lidmaatschap en onderwijs weigeren. Zij kunnen onze toegang tot het goede leven beperken.'[92]

'Kennis is macht,' luidt het gezegde. Na onze zoektocht concluderen wij: informatie- en kennisongelijkheid is machtsongelijkheid. Op individueel niveau kunnen daarvan de gevolgen groot zijn. Maar niet alleen op individueel niveau: deze machtsongelijkheid heeft de potentie om een maatschappij te ontwrichten. Fundamentele waarden als het non-discriminatiebeginsel, de onschuldpresumptie en solidariteit kunnen erdoor onder druk komen te staan.

Ja, dat zijn grote woorden, maar het voorbeeld van de Amerikaanse rechters die hun straffen deels af laten hangen van automatisch gegenereerde risicoscores laat zien dat het mogelijk is. Want zwarten blijken daardoor in Amerika zwaarder bestraft te worden dan witten die een vergelijkbare misdaad hebben begaan.

Of wat te denken van de invloed van datagedreven bedrijven op het politiek debat en de publieke opinie? De onderzoeken naar de potentiële macht van Facebook en Google om verkiezingsuitslagen te manipuleren zijn een veeg teken.

Een blik op de toekomst

Tot nu toe zijn wij met beide benen op de grond blijven staan; nu is het tijd om even op te stijgen. Als we die macht en machtsongelijkheid op dit moment nog niet kraakhelder kunnen zien, als wij enkel nog wat rimpelingen ontwaren van wat er onder de oppervlakte plaatsvindt, dan kan een blik op de toekomst helderheid bieden.

De bekende privacyactivist Brad Templeton nam zijn toehoorders eens mee in een fascinerend gedachte-experiment. Stel je voor, zei Templeton, dat het in de toekomst mogelijk is dat robots kunnen tijdreizen. Zij komen naar het heden om ons te bestuderen en brengen de datatechnologie van de toekomst mee: hardware, software en analysemethoden die zo geavanceerd zijn, dat wij ons ze nu niet kunnen voorstellen. Wat gebeurt er dan? De robots zijn in staat om er alle data die ze van ons kunnen vinden mee te analyseren en te gebruiken. Wat ze met onze gehele datageschiedenis kunnen is letterlijk onvoorspelbaar. Maar, zegt Templeton, *wij* kunnen niet tijdreizen en onze data uit het verleden verwijderen.[93]

Dit klinkt misschien als een vage denkoefening, maar het punt is dat dit onze werkelijkheid beschrijft. Wij genereren enorme bakken data die nooit meer verdwijnen. De technologieën om die data te analyseren worden met de dag geavanceerder. Wij hebben geen idee welke conclusies er door de algoritmes van de toekomst worden getrokken. We hebben geen idee welke informatie die nu nog privaat is plotseling openbaar wordt. We weten niet wat de software en databases straks met onze data kunnen. We kennen de toekomst niet.

Ook op een niet-technologisch niveau weten wij niet hoe andere partijen dan met onze data zullen omgaan. We beschreven al dat technologiebedrijven geregeld hun privacyvoorwaarden aanpassen en daarmee de 'afspraak' die het bedrijf op moment X met miljoenen klanten maakte, op moment Y eenzijdig opzegde. De geschiedenis van Facebook en Google toont een boulevard van verbroken beloften. Dit betekent dat hoogstwaarschijnlijk jouw data in de toekomst op andere manieren gebruikt zullen worden dan de manier die jou beloofd is op het moment dat je klant werd van het bedrijf.

En bij het gebruik van gegevens ligt altijd de glijdende schaal op de loer: als bepaalde data toch al voor functie A zijn verzameld, waarom zouden ze dan niet ook voor functie B kunnen worden

gebruikt? En C en D? *Function creep* wordt dit genoemd. Het fundamentele probleem daarvan is dat je als burger of consument de nieuwe functies die jouw gegevens krijgen op geen enkele manier aan kunt zien komen. Je weet wat er met jouw gegevens gebeurt op moment X, maar het toekomstig gebruik op moment Y laat zich niet voorspellen.

Parkeergegevens stellen de Belastingdienst in theorie in staat om van iedere autorijder te kunnen achterhalen waar hij de nacht heeft doorgebracht. Het is op dit moment misschien onvoorstelbaar dat de Belastingdienst daar gebruik van zal maken of er überhaupt in geïnteresseerd is, toch is het naïef om te denken dat dit in de toekomst niet zou kunnen veranderen.

Dat laat ook het verhaal van de familie Van der Ziel uit Delfzijl zien, waar we dit boek mee begonnen. In de jaren zeventig vonden zij de vooroorlogse administratie van de plaatselijke Joodse gemeenschap in een schuilplek op hun zolder. Het ging om volstrekt onschuldige notities over familieverbanden, brieven en andere dagelijkse zaken. Die administratie was daar na het uitbreken van de oorlog door een rabbijn verstopt. De rabbijn wist dat deze gegevens in handen van de Duitsers van betekenis zouden veranderen. Het is niet bekend of de actie van de rabbijn levens heeft gered. Zijn verstopactie maakt desondanks duidelijk: gegevens kunnen, als ze in de toekomst in verkeerde handen vallen, opeens dodelijk zijn.

Het verhaal van de rabbijn uit Delfzijl is verwant aan dat van de aanslag op het Amsterdamse Bevolkingsregister in 1943, een verhaal dat niet vaak genoeg verteld kan worden. De gemeente Amsterdam had in de jaren dertig een ongekend gedetailleerd archief opgetuigd met daarin persoonlijke informatie over alle Amsterdammers: hun namen, adressen, relaties en beroepen. Met de allerbeste bedoelingen opgezet, om de gemeente efficiënter te maken. In 1940 bleken die goede bedoelingen een keerzijde te hebben: ook ieders religie en etniciteit stonden in de databank vermeld. Iedere Amsterdamse Jood was in de databank

terug te vinden. Wat was opgezet als een goedbedoeld project, werd in één klap een databank des doods. Reden voor het zogenoemde Kunstenaarsverzet, onder aanvoering van Gerrit van der Veen, om de archieven met benzol en trotyl te overgieten en in brand te steken.

We hebben lang getwijfeld of we de Tweede Wereldoorlog erbij moeten halen. We kunnen ons voorstellen dat lezers dan denken: 'Ach dat is zo lang geleden, die tijd is voorbij.' Of: 'We leven in een democratie, nu kan dat niet meer gebeuren.'

Wij zijn daar niet zo zeker van. Iedere zittende macht maakt uiteindelijk plaats voor een andere. Op het moment dat wij dit schrijven, in de zomer van 2016, zijn in Europa politieke partijen in opkomst die er behoorlijk autoritaire denkbeelden op nahouden. In Finland, Zweden, Denemarken, Nederland, België, Frankrijk, Portugal, Oostenrijk, Polen, Tsjechië, Hongarije en Griekenland boeken zij electorale successen. Zonder een oordeel te vellen over hun politieke ideologieën: wat als het door hen beloofde repressieve beleid – waarvan een deel ongetwijfeld verkiezingsretoriek is – straks werkelijkheid wordt? Wat zullen de gevolgen zijn voor de minderheden waar zij zo kritisch op zijn? Of voor andere groepen waar zij hun pijlen op richten – journalisten van de publieke omroep, in het geval van de PVV bijvoorbeeld – als deze leiders van de toekomst over de data en systemen van nu beschikken?

Eenzelfde redenering gaat op voor technologiebedrijven. Ooit zal iemand het stokje van Mark Zuckerberg overnemen en de leiding krijgen over Facebook. Hetzelfde geldt voor Larry Page en Sergey Brin van Google. Hun opvolgers kunnen doorgaan op dezelfde voet als zij, ze zouden ook volledig van koers kunnen veranderen. Misschien gaan hun aandeelhouders wel eisen dat er iemand aan het roer komt die nog méér economisch gewin kan halen uit onze data. Misschien wordt het bedrijf wel overgenomen. En wat gebeurt er met onze data als Facebook failliet gaat?

Ook relevant om te realiseren als wij het *nu* over onze data hebben: wetten zijn niet statisch, ze veranderen altijd. Wat nu illegaal is, kan morgen legaal zijn, en andersom. Neem homoseksualiteit. Tot niet eens zo heel lang geleden was het in alle westerse landen verboden om een relatie met iemand van hetzelfde geslacht te hebben. In het Verenigd Koninkrijk werden mannen tot in de jaren vijftig chemisch gecastreerd als bekend was dat ze homoseksueel waren.

Andersom: er is een gerede kans dat het eten van vlees over vijftig jaar gecriminaliseerd is. Net als roken. Het grote verschil met vroeger is dat de hedendaagse technologie de belofte van perfecte handhaving in zich draagt. Die belofte van: er zijn nu zoveel data en er zijn zulke geavanceerde analysemethoden, dat wij daadwerkelijk ongewenst gedrag kunnen detecteren, voorspellen en uiteindelijk *voorkomen.*

Wanneer je bedenkt hoeveel data er nu al van ons rondzwerven, dan roept dit, met het oog op de toekomst, een aantal ongemakkelijke vragen op. Wat zijn de consequenties voor al die miljoenen mensen van wie nu al foto's online rondzwerven terwijl zij een sigaret in hun hand hebben of in een hamburger bijten, als roken en vlees eten straks mogelijk illegale activiteiten zijn? Of wat betekent het voor mensen die nu als delinquenten en pas later als revolutionairen worden gezien?

Dat dit geen hypothetische gedachtegang is, kwam in mei 2016 aan het licht. Toen bleek dat de CIA decennia geleden cruciale informatie over de verblijfplaats van Nelson Mandela aan de Zuid-Afrikaanse inlichtingendienst had gegeven. Deze informatie leidde in 1962 tot zijn arrestatie en gevangenschap, dat meer dan 27 jaar zou duren. Mandela werd beschouwd als een groot gevaar – óók door de Verenigde Staten. Een betrokken CIA-agent motiveerde zijn daad in een documentaire en noemde Mandela 'de gevaarlijkste communist van de wereld buiten de Sovjet-Unie.' Dertig jaar later ontving Mandela de Nobelprijs voor de Vrede. Nu wordt de Zuid-Afrikaanse ex-president gezien als een van de

grootste vrijheidsstrijders van de twintigste eeuw – ook in de Verenigde Staten.

Met andere woorden: de definities van 'terrorist,' 'vijand' of 'gevaar voor de nationale veiligheid' kunnen volledig veranderen. Toch zijn het precies die woorden waar geheime diensten mee werken en die bepalen over wie zij data verzamelen, op wie zij extra surveillance richten en wie er, pak 'm beet, op een No-Fly List terechtkomt.

In zijn boek *To Save Everything, Click Here* poneert technologiedenker Evgeny Morozov een interessante gedachte over de Verenigde Staten van eind jaren zestig. In de bussen van toen waren de zitplaatsen achterin bedoeld voor de zwarten en de plekken voorin voor de witten. De zwarte activiste Rosa Parks besloot op een dag voorin te gaan zitten, als een daad van verzet. Als gevolg hiervan braken er rellen uit die uiteindelijk tot de afschaffing van de segregatiewetten leidden. Wat, vraagt Morozov zich af, als bussen eind jaren zestig sensoren en gezichtsherkenningssoftware zouden hebben. 'Zou het ons een Rosa Parks hebben gegeven? Waarschijnlijk niet, want zij zou niet eens voorin de bus hebben kunnen gaan zitten.'

De neiging van bedrijven en overheden om wenselijk gedrag met behulp van nieuwe technologieën te voorspellen, beïnvloeden en voorkomen, kan als gevolg hebben dat gedrag wordt opgelegd dat over dertig jaar als onwenselijk wordt gezien, of dat gedrag dat later als heldhaftig of zelfs revolutionair wordt beschouwd, in de kiem wordt gesmoord.

Waar blijft de tegenmacht?

Dit brengt ons op de belangrijkste conclusie van onze zoektocht. Als privacy uiteindelijk over macht gaat, dan heeft de huidige én toekomstige macht tegenmacht nodig. Tegenmacht die deze

machten kritisch bevraagt, blootlegt, weerspreekt, tegenwerkt als ze te ver dreigen te gaan, inperkt als ze te groot dreigen te worden en sanctioneert als ze over de schreef gaan.

Voor de lezer die nu een pasklaar antwoord verwacht: dat antwoord gaat niet komen. De hoofdstukken in dit boek tonen hoe breed en veelkoppig het probleem is. Het is én politiek én juridisch én maatschappelijk én ethisch én technologisch én economisch een probleem. Tegenmacht zou zich navenant op al deze niveaus moeten manifesteren. En dat is gemakkelijker gezegd dan gedaan.

Dus, wat te doen? Die vraag krijgen wij altijd na publicatie van onze stukken. Hoe kan ik mijzelf wapenen tegen de datagraaiers? Welke maatregelen moet ik nemen?

Omdat we het privacyprobleem in zijn volle glorie wilden beschrijven, hebben wij er bewust voor gekozen om hiervoor niet in te gaan op tegenmaatregelen en digitale zelfverdedigingstrucs.

Die zijn er wel. Dat begint klein, met een bewustere omgang met onze data. We kunnen ad blockers gebruiken om tracking cookies te blokkeren. We kunnen onze digitale en online veiligheid verbeteren: sterke wachtwoorden kiezen, niet zomaar inloggen op een onbeveiligd netwerk, goed waken over onze en andermans data. Op de site van *De Correspondent* [corr.es/zelfverdedigingsgids] hebben wij een zelfverdedigingsgids in elkaar gezet, zodat je kunt zien welke maatregelen voor jou geschikt zijn.

We kunnen – ondanks alle praktische en inhoudelijke bezwaren – inzageverzoeken doen bij bedrijven en overheden. Hun vragen wat zij van ons weten en wat zij met die informatie doen. We kunnen van onze bazen eisen dat ICT- en databeveiliging de hoogste prioriteit krijgen.

We kunnen organisaties steunen die strijden tegen onnodige surveillance en voor privacy. Doneren aan burgerrechtenorganisaties Bits of Freedom, Amnesty International of Privacy First. We kunnen ons verdiepen in politieke partijprogramma's en beoordelen welke partijen de beste plannen en ideeën over privacy en surveillance hebben.

Als wij naar wat grotere trends kijken, dan zijn er hoopgevende ontwikkelingen te ontwaren. Er wordt al tegenmacht geboden.

Op *politiek niveau* heeft het Europees Parlement in het voorjaar van 2016 nieuwe wetgeving aangenomen voor de gegevensbescherming van alle inwoners van de hele Europese Unie. Daarin staat, onder meer, dat privacytoezichthouders meer middelen krijgen om bedrijven te dwingen zich aan nationale wetgeving te houden. Gedragsgegevens worden (iets) beter beschermd. Mensen krijgen (iets) meer controle over hun data.

Ook heeft de Europese Commissie Google volop in het vizier. Er lopen meerdere onderzoeken naar mogelijk machtsmisbruik van het bedrijf op het eigen advertentienetwerk, het mobiele besturingssysteem Android en de eigen prijsvergelijker. De mogelijke boete kan oplopen tot 10 procent van de jaarlijkse omzet van het bedrijf.

Op *technologisch niveau* zetten veel grote internetbedrijven sinds de onthullingen van Snowden in op de beveiliging van gegevens en communicatie van hun klanten. Apple vocht publiekelijk met 's werelds machtigste opsporingsdienst FBI om de overheid geen toegang te geven tot ieders iPhone 5. Google introduceerde *end-to-end*-encryptie, zodat de inhoud van communicatie wordt afgeschermd – ook voor Google zelf. Berichtendienst WhatsApp deed dat ook, waardoor de appjes van meer dan een miljard gebruikers beveiligd zijn.

WhatsApp maakt daarbij gebruik van dezelfde technologie als Signal – een steeds populairder wordende chat-en-belapp die door experts als zeer veilig wordt gezien en die stukken gebruikersvriendelijker is dan andere versleutelingsprogramma's.

Een andere positieve ontwikkeling is de enorme populariteit van ad blockers – naar schatting zijn er in juni 2016 meer dan honderd miljoen gebruikers van deze simpele software die online advertenties weert. Een positief neveneffect van de meeste ad blockers is dat ze trackers buiten de deur houden.

Op *intellectueel niveau* is een aantal serieuze technologiedenkers de afgelopen jaren doorgedrongen tot de mainstreammedia. Hun fundamentele kritiek op surveillance bereikt een veel groter publiek dan voorheen. Een aantal van hen speelt ook in dit boek een rol, onder wie Evgeny Morozov, Shoshana Zuboff en Bruce Schneier.

Tegelijkertijd worden serieuze rapporten en analyses over privacy en surveillance steeds beter opgepikt door journalisten. Het doorwrochte rapport over Big Data van de WRR bijvoorbeeld waar wij in hoofdstuk drie over schreven. Of een zeer kritische analyse van de Global Commission on Internet Governance, bestaande uit een aantal invloedrijke (ex-)politici en oud-medewerkers van de inlichtingendiensten.[94]

De journalistiek heeft zich de afgelopen jaren bekwaamd in thema's als technologie, surveillance en privacy. In Nederland waren dit tot voor kort ondergeschikte journalistieke onderwerpen; nu besteden de grote nieuwszenders er met regelmaat aandacht aan en hebben kranten enkele van hun beste onderzoeksjournalisten vrijgemaakt om zich erop te storten.

Ook vermeldenswaardig is dat het Europese Hof van Justitie in Luxemburg zich heeft opgeworpen als een belangrijke rechterlijke beschermheer van privacy als mensenrecht – met name in twee belangrijke uitspraken. In 2014 oordeelde het Hof dat de EU-lidstaten niet zomaar alle telecomgegevens mogen bewaren voor opsporingsdoeleinden. Het afwijzen van deze zogenoemde dataretentierichtlijn was een rigoureuze breuk met het verleden.

In oktober 2015 zette het Hof bovendien een streep door het zogenoemde *Safe Harbour*-verdrag tussen de Europese Unie en de Verenigde Staten. In dit verdrag stond onder welke voorwaarden data van EU-burgers naar Amerikaanse bedrijven mochten worden verzonden. Het Hof oordeelde dat Amerikaanse bedrijven helemaal niet in staat waren om de data van Europeanen te beschermen tegen de NSA en dwong met zijn uitspraak de Verenigde Staten en de Europese Unie terug naar de onderhandelingstafel voor een nieuw verdrag.

De krachten zijn enorm

Opgelost dus? Nee, bij lange na niet. Zonder deze ontwikkelingen en individuele maatregelen direct af te serveren als nutteloos – dat zijn ze echt niet – kunnen we met volle overtuiging zeggen dat het slechts druppels op een gloeiende plaat zijn. Achter de datahonger van overheden en bedrijven schuilen te grote krachten. De wens tot sociale beheersing onder politici en overheden zal niet zomaar afnemen.

Nota bene op dezelfde dag dat het Europees Parlement de nieuwe wetgeving voor de gegevensbescherming aannam, stemde het óók voor de invoering van controversiële wetgeving die de uitwisseling van boekingsinformatie mogelijk maakt. Vanaf 2018 worden alle vlieggegevens van iedereen die Europa in- of uitvliegt jarenlang bewaard en gebruikt voor profiling. En ja, grote technologiebedrijven investeren in de beveiliging van de data van hun gebruikers, maar hun honger naar meer en meer data is ongelimiteerd. Het verdienmodel van technologiebedrijven, surveillancekapitalisten en datamakelaars gaat niet opeens veranderen. In de tussentijd denderen de technologische ontwikkelingen op het gebied van surveillance voort – wat is er *niet* smart tegenwoordig?

Het publieke debat over privacy is weliswaar recent naar een hoger niveau getild, daartegenover staan politici die zich hier weinig van aantrekken. Denk alleen al aan het voorstel van de Nederlandse kaderwet gegevensuitwisseling, die er in het kort op neerkomt dat privacywetgeving opzij wordt geschoven en meer databases aan elkaar worden gekoppeld om fraude te bestrijden.

En de vernietigende uitspraak van het Hof over het Safe Harbour-verdrag was indrukwekkend, maar het resultaat – *nieuwe* afspraken tussen de Europese Unie en de Verenigde Staten over gegevensuitwisseling – wordt door iedereen met een beetje verstand van de materie als slappe hap beschouwd. De verwachting is dat het Hof ook dit verdrag zal afwijzen, maar daar is eerst weer een lang juridisch proces voor nodig.

En laten we ons eigen gedrag als consument en burger niet vergeten. Het is verleidelijk om de schuld af te schuiven op de Grote Boze Bedrijven en Overheden, maar laten we eerlijk zijn: wij zijn degenen die zo gretig gebruikmaken van al die zogenaamd gratis diensten en die korting willen op verzekeringspremies in ruil voor onze gedragsgegevens. Wij zijn degenen die, als het erop aankomt, denken dat we niets te verbergen hebben.

En nu?

Wij zijn somberder geworden door deze zoektocht. Er is een omwenteling nodig. We moeten fundamenteel anders over data en privacy gaan praten. Ongebreidelde surveillance die buiten het zicht om plaatsvindt en die leidt tot ondoorzichtige invloed op ons leven, vormt een bedreiging voor fundamentele kernwaarden als burgerschap, autonomie en democratie. Privacy is een essentieel collectief goed. Het gaat over ons allemaal. Alleen als dit besef echt doordringt, kan er vruchtbare grond ontstaan waar échte duurzame tegenmacht georganiseerd kan worden.

Ik heb niets te verbergen, zeg je?

Wij hebben heel veel te beschermen.

Epiloog

Een nieuw privacyklimaat

Het is zonneklaar: het gesprek over privacy moet veranderen. De 'ik heb niets te verbergen'-houding moet plaatsmaken voor een collectief besef dat wij veel te beschermen hebben. Pas dan kunnen wij weerstand bieden aan de krachten die onze privacy – en daarmee waarden als burgerschap, solidariteit en autonomie – in gevaar brengen.

Hoe dat te realiseren? In gesprekken met denkers en wetenschappers kregen wij meermaals het advies eens naar dat andere veelkoppige probleem te kijken: de opwarming van de aarde. Het klimaatprobleem is de afgelopen jaren wel op de agenda komen te staan.

De belangrijkste verklaring hiervoor is dat we het klimaatprobleem sinds de jaren negentig als een collectief probleem zijn gaan zien. Voor die tijd was het gebruik van fossiele energie voornamelijk een economische kwestie. Overheden, bedrijven en consumenten verbruikten zoveel als zij konden betalen. Eind jaren tachtig ontstond het besef dat we met ons fossiele-energiegebruik een stabiel leefklimaat konden vernietigen en in de jaren negentig werd de eerste wereldwijde klimaattop georganiseerd. In 2006 wist Al Gore met zijn film *An Inconvenient Truth* de aandacht van de wereld op de opwarming van de aarde te richten en vorig jaar werd het ambitieuze Akkoord van Parijs gesloten, waarbij alle landen van de wereld opnieuw de intentie uitspraken de opwarming van de aarde tot maximaal 2 graden Celsius te beperken. Verder is het voor de politiek en het bedrijfsleven zo langzamerhand on-

mogelijk geworden geen aandacht aan het klimaatprobleem te besteden. En zijn burgers in grote meerderheid voorstander van streng klimaatbeleid en groene energie geworden. Hoewel we nog steeds op een gevaarlijke klimaatverandering van meer dan 2 graden Celsius afstevenen, is inmiddels ook een wereldwijde overschakeling naar duurzame energie op gang gekomen.

Op het eerste oog lijkt het nogal vergezocht om de privacydiscussie en de klimaatdiscussie met elkaar te vergelijken. De opwarming van de aarde levert directe gevaren op voor mensen die worden getroffen door de stijgende zeespiegel of door extreem weer. In de klimaatdiscussie gaat het over oorlog en vrede, leven en dood. Dat is bij privacy niet het geval, of in ieder geval niet zo duidelijk als bij het klimaat.

Als we de privacydiscussie en de klimaatdiscussie door een andere bril bekijken, zien we ook overeenkomsten. Het zijn allebei abstracte problemen; als iedereen om je heen het probleem negeert, ben jij geneigd dat ook te doen; de mogelijke 'rampen' liggen voor de meesten van ons ergens in de toekomst; we zien de oorzaken van de opwarming van de aarde en het privacyverlies niet met het blote oog – dataverzameling en -gebruik vinden onder de oppervlakte plaats, CO2-uitstoot is onzichtbaar; en bovendien begrijpen we er eigenlijk maar bar weinig van. Wie snapt de risico's van het opbreken van het ijs op Antarctica nu echt? En wie weet wat er in zijn smartphone gebeurt?

Beide zijn, kortom, problemen die wij makkelijk kunnen negeren. Toch is de klimaatbeweging erin geslaagd de opwarming van de aarde als een collectief en moreel probleem neer te zetten. Waardoor er nu iets aan het veranderen is. Hoe is dat gelukt?

Met collega Jelmer Mommers, de klimaatjournalist van *De Correspondent*, gaan we te rade bij enkele prominente klimaatstrijders. De vragen die wij hun voorleggen: Wat heeft ervoor gezorgd dat het klimaat als een collectief probleem zo prominent op de agenda is komen te staan? En welke lessen zijn daar voor de privacybeweging uit te leren?

Voor de goede orde: het gaat ons niet om een blauwdruk of een uitputtende analyse. Eerder is het een verkenning, een gedachte-experiment waar aanknopingspunten uit voort kunnen vloeien.

1 Benoem vijanden waar mensen zich collectief tegen kunnen verzetten

Hoe moeten degenen die privacy willen opstoten in de vaart der volkeren – politici, non-gouvernementele organisaties, activisten en journalisten – het probleem brengen?

We leggen het voor aan een autoriteit op het gebied van klimaatcommunicatie: George Marshall. Hij werkte 25 jaar lang voor de milieubeweging, onder meer bij Greenpeace en de Amerikaanse Rainforest Foundation, en richtte daarna een denktank voor klimaatcampagnes op. Hij verzamelde zijn kennis in het boek *Don't Even Think About It: Why Our Brains Are Wired to Ignore Climate Change.*[95] Daarin beschrijft hij de psychologie van klimaatverandering en zoekt hij manieren om meer mensen bewust te maken van de risico's.

Bij klimaatverandering is een sleutel tot het voorlopige succes het creëren van vijanden geweest, vertelt Marshall. Kolenboeren en bedrijven als ExxonMobil en Shell tot slechteriken verklaren – en dan mensen mobiliseren.

Daar liggen zeker kansen voor de privacybeweging, denkt Marshall. Een gemeenschappelijke vijand verbroedert. 'Niemand voert echt agressief campagne tegen Facebook. Terwijl dit soort grote organisaties extreem kwetsbaar zijn voor campagnes, omdat ze financieel totaal overgewaardeerd zijn. Ze zijn alleen wat waard als mensen Facebook blijven gebruiken.'

2 Ken je publiek en pas daar de boodschap op aan

Dat moet niet het enige zijn, zo luidt het advies van Marshall. 'Mijn indruk is dat veel privacyactivisten links en antibedrijfsleven zijn. Hun wereldbeeld is: deze multinationals willen hun macht uitbreiden en geld verdienen en daarom proberen ze het internet over te nemen.' Veel argumenten in het privacydebat nemen volgens Marshall de vorm aan van kapitalismekritiek of pleidooien voor sociale rechtvaardigheid.

En daar gaat het mis, weet hij, want bij klimaatverandering zijn het precies dat soort argumenten geweest waardoor veel conservatieve en rechtse mensen zich van het onderwerp afwendden. Als je de boodschapper niet vertrouwt, vertrouw je ook zijn probleemstelling en zijn oplossingen niet. In Amerika wordt klimaatverandering door sommigen zelfs gezien als een links complot om de macht van de overheid te vergroten of zelfs een socialistische heilstaat te rechtvaardigen.

Dat gevaar loert ook voor privacyactivisten, meent Marshall. Tenminste: als zij niet óók een verhaal hebben voor de mensen en partijen van buiten de eigen parochie. Zo zullen klassiek liberalen meer aanslaan op de boodschap dat surveillance door overheden hen in hun autonomie en vrijheid beknot dan een verhaal over Facebook als grote surveillancekapitalist.

3 Grote groepen mobiliseren is makkelijker met hoopvolle toekomstscenario's

Technologiecriticus Evgeny Morozov vindt dat we niet bang genoeg zijn voor de gevolgen van de inperking van onze privacy. Het probleem, meent hij, is dat we ons het privacyequivalent van een mogelijke klimaatcatastrofe – de 'informatieapocalyps' – nauwelijks kunnen voorstellen. 'Wij zijn erg slechte dystopisten geworden en onze technofiele intellectuelen zijn daar deels verantwoordelijk voor,' aldus Morozov.

Nog even los van het feit dat een informatieapocalyps ook daadwerkelijk moeilijker voor te stellen is dan een klimaatapocalyps – denk: massamigratie en ontwrichting door droogte, voedselgebrek en de stijgende zeespiegel – trekken sommige klimaatdenkers ook de effectiviteit van dergelijke door Morozov voorgestelde dystopieën in twijfel.

Sterker nog: mensen bang maken, benadrukken zij, is een slechte strategie. Want bange mensen zijn passief en vinden geen oplossingen. Weinig verhalen hebben het klimaatdebat zo verstard en gepolariseerd als 'het verhaal van de apocalyps van de klimaathel,' schrijft de Noorse psycholoog Per Espen Stoknes in *What We Think About When We Try Not To Think About Global Warming: Toward a New Psychology of Climate Action.*[96] Mensen mobiliseren rond hoopvolle toekomstscenario's zou beter werken, denkt hij.

4 Trek wel lijnen

Toch heeft het schetsen van een doemscenario één voordeel, leren wij van George Marshall. Het laat namelijk zien dat er ergens harde grenzen gesteld moeten worden, omdat we anders, zonder dat we het doorhebben, langzaam in een dystopische situatie afglijden – en dan zijn we te laat om nog in te grijpen.

'De klimaatbeweging moest ook grenzen stellen,' zegt Marshall. Op de klimaatconferentie in Parijs eind 2015, en bij een wereldwijde mobilisatie van burgerlijke ongehoorzaamheid in mei 2016, werd daarom campagne gevoerd rond het idee van een 'rode lijn': tot hier en niet verder. Die lijn moest de harde 'grens' van de natuur en de kwetsbaarste gemeenschappen op aarde vertegenwoordigen. Kwetsbare eilandstaten voerden zo campagne met de leus: '*1.5 to stay alive*' – meer dan 1,5 graad Celsius zou hun doodvonnis betekenen. Politici en fossiele-energiebedrijven mochten die grens niet overschrijden en moesten een ambitieus akkoord sluiten zodat gevaarlijke klimaatverandering zou uitblijven.

Het bleek een effectieve boodschap: in het Akkoord van Parijs werd afgesproken de opwarming te beperken tot 'ruim beneden' 2 graden Celsius, met een 'streven' niet boven 1,5 graad uit te komen (al moet gezegd worden dat het beleid om die ambitie waar te maken vooralsnog ontbreekt).

'Je moet duidelijk maken welke verandering onacceptabel is,' zegt Marshall. 'Dat is de kern van campagne voeren. Ik denk dat hier een echte kans ligt. Hét argument kan zijn: er is nu in feite geen grens aan de informatie die bedrijven en overheden kunnen verzamelen. Dus die grens moeten we trekken.'

5 Ga voor het allerhoogste politieke niveau

Harde grenzen hebben nog een voordeel: ze geven machthebbers een referentiepunt. Ze concretiseren de strijd over ontwikkelingen die wel en niet wenselijk zijn. Dat geldt met name voor de internationale politiek, omdat privacy en klimaat zich van landsgrenzen weinig aantrekken. Denk aan inlichtingendiensten die internationaal opereren en persoonlijke gegevens met elkaar uitwisselen, technologiebedrijven die overal ter wereld hun servers hebben staan en Europese privacywetgeving die voor alle EU-landen geldt.

We bellen met Bas Eickhout, sinds 2009 Europarlementariër namens GroenLinks. Eickhout is in Brussel een gevierd voorvechter van duurzaamheid. Zijn grootste politieke overwinning haalde hij eind 2013, toen hij erin slaagde een strenge wet aanvaard te krijgen om het gebruik van krachtige broeikasgassen – de zogenoemde F-gassen – terug te dringen in onder meer koelkasten en airconditioners.

Ten eerste, zegt Eickhout, kan het doorslaggevende politiek belang van de Verenigde Naties voor de strijd voor het klimaat niet genoeg benadrukt worden. De VN hebben een enorme bureaucratie opgetuigd – de United Nations Framework Convention on Climate Change (UNFCCC) – om jaarlijks met de hele wereld over

het klimaat te praten. 'Klimaat is echt een geïnstitutionaliseerd onderwerp binnen de VN. Daardoor heeft het enorm veel gewicht; iedere nationale overheid zet er ambtenaren op. Dat dwingt politici weer om daar aandacht aan te besteden. De VN zijn natuurlijk bureaucratisch, maar alleen al dat er een jaarlijkse klimaattop is en dat men jaarlijks op het hoofdkantoor van de UNFCCC in Bonn samenkomt, heeft veel positieve effecten. Want daar gaan óók de ambtenaren van elk milieuministerie uit alle landen naartoe, die daar weer met de neus op de feiten gedrukt worden, wat ze weer terugkoppelen naar hun ministers. Dat is – puur politiek gezien – heel belangrijk.'

Eickhout noemt nog een meerwaarde van de VN. Aandacht voor onderwerpen als klimaat en privacy is altijd afhankelijk van de actualiteit. Zo stond privacy prominent op de agenda na de onthullingen van Edward Snowden, om daar vervolgens met evenveel gemak weer van te verdwijnen na enkele terroristische aanslagen. Eickhout: 'Bij het klimaat is de politieke aandacht ook jarenlang als een pendule geweest. Dan had je een ramp en zat het mee, en vervolgens kwam er een 'sceptische golf' en zat het weer tegen. Maar door dat institutionele proces is er een gestaag stijgende lijn gekomen, waar die pendule omheen bewoog. Zonder die stijgende lijn blijft het een herhaling van zetten.'

Eickhout juicht het toe dat de Verenigde Naties vorig jaar in juli een rapporteur voor het recht op privacy hebben aangesteld. 'Een goede eerste stap,' zegt hij. Maar nog ver verwijderd van de duizenden VN-ambtenaren die zich buigen over de opwarming van de aarde. 'Het risico is dat het onderwerp zo een beetje wordt weggestopt en politici denken: het is afgehandeld.'

Wat zou die rapporteur moeten doen? Eickhout: 'Het mooiste zou zijn als het hem lukt om de landen van de wereld op één lijn te krijgen over gemeenschappelijke ambities rond het behoud van privacy, zoals dat gebeurde in 1992, toen alle landen van de wereld met elkaar afspraken om gevaarlijke klimaatverandering te voorkomen. Dat hebben ze vooralsnog niet helemaal waargemaakt,

maar ze kunnen nu wel op het matje worden geroepen als ze hun eigen ambities in de wind slaan.'

6 Span processen aan voor de collectieve zaak

Advocaat Roger Cox won met de actieorganisatie Urgenda de inmiddels wereldberoemde klimaatzaak tegen de Nederlandse staat. Die werd verplicht om de uitstoot in 2020 met ten minste 25 procent terug te dringen.

Cox' strategie was als volgt. Alle landen van de wereld hadden in 1992 afgesproken dat ze gevaarlijke klimaatverandering wilden voorkomen. Later werden ze het erover eens dat een opwarming van meer dan 2 graden Celsius 'gevaarlijk' was en uit de klimaatwetenschap volgt dat rijke landen hun uitstoot daarom in 2020 met zeker 25 procent moesten terugbrengen ten opzichte van 1990. Via de rechter dwong Cox die door Nederland verzaakte reductie alsnog af.

Is een vergelijkbare strategie te volgen voor het afdwingen van een betere bescherming van onze privacy? Is aannemelijk te maken dat er een punt bestaat waarna effecten optreden die niet meer terug te draaien zijn? Want dan zou de overheid op basis van haar zorgplicht nu al moeten ingrijpen.

Cox ziet wel aanknopingspunten. Als sprake is van machtsasymmetrie – zoals tussen de aanbieder en de gebruiker van een online dienst – is het recht een goed middel om bescherming af te dwingen. Als individu sta je relatief zwak ten opzichte van grote technologische ontwikkelingen en multinationals die jouw autonomie aantasten, analyseert Cox, dus in principe zal de rechter geneigd zijn jou in concrete gevallen te beschermen.

Privacyjuristen zullen wel op zoek moeten gaan naar zaken waar ze dit algemene principe hard kunnen maken. 'Eigenlijk kunnen alleen juristen die de hele ICT-wereld begrijpen dit doen,' zegt Cox. Bovendien moeten ze – als ze zich net als Cox willen beroepen op het voorzorgsprincipe – goed duidelijk maken wat het gevaar is waartegen burgers beschermd moeten worden. Cox: 'Wat is het gevaar van metadata? Vinden we dat maatschappelijk onaanvaardbaar?' Als dat lukt, kan in principe een zaak gemaakt worden die de staat dwingt nu al in te grijpen.

Privacy heeft daarbij één voordeel ten opzichte van het klimaat: het is een grondrecht. Het klimaat is dat niet en moet in rechtszaken vertaald worden naar andere grondrechten, bijvoorbeeld het grondrecht op voedsel. Privacyadvocaten kunnen proberen dat grondrecht te gebruiken om bij de rechter 'positieve verplichtingen' af te dwingen waar overheden en bedrijven aan moeten voldoen. Staten kunnen dan verplicht worden wetten in te voeren die bedrijven dwingen de privacy van consumenten goed te bewaken.

Dit gebeurde in oktober 2015 in een rechtszaak die door juristen als revolutionair wordt gezien. De Oostenrijkse privacyactivist Max Schrems won een zaak die hij had aangespannen voor het Europese Hof van Justitie over het Safe Harbour-verdrag tussen de EU en de Verenigde Staten over de uitwisseling van persoonsgegevens. Het Hof oordeelde met een beroep op het Europees Verdrag voor de Rechten van de Mens dat dit verdrag niet wettig was.

7 Centraliseer de wetenschap van privacy en surveillance

Van verschillende kanten horen wij over de grote invloed van het Intergovernmental Panel on Climate Change (IPCC). Dat is een wetenschappelijk orgaan dat in 1988 werd opgericht door de Verenigde Naties. Bij het IPCC zijn honderden experts van over de hele wereld aangesloten. Zij overzien de vele honderden studies die de klimaatwetenschap voortbrengt. Om de vijf à zes jaar publiceert het IPCC een samenvatting van alle literatuur over het klimaatprobleem.

Advocaat Roger Cox baseerde zijn strategie in de klimaatzaak voor een belangrijk deel op de uitgebreide studie van de IPCC-rapporten. 'Volgens het IPCC zou een groep 'rijke landen' voor 2020 tussen de 25 en 40 procent van de uitstoot gereduceerd moeten hebben ten opzichte van 1990, om een redelijke kans te houden dat we de 2 graden Celsius niet overschrijden. Ik beargumenteerde dat als het om de bewijsvoering gaat, we alleen op het IPCC kunnen afgaan. Niemand bracht daar iets tegenin.'

Ook politiek is het IPCC doorslaggevend geweest, meent Europarlementariër Bas Eickhout.

'Interessant is dat de samenvatting van het IPCC een politiek goedgekeurde samenvatting is. De politiek kan het probleem daarna moeilijk meer ontkennen.' Dat heeft er volgens Eickhout voor gezorgd dat klimaat steeds belangrijker is geworden in de politiek. 'Dat iedereen het over het klimaat heeft, komt deels door het IPCC. Politiek is het een thema waar je het liefst omheen wil wandelen, maar dat kan gewoon niet meer. Het IPCC herinnert de politiek steeds weer aan de opwarming van de aarde.'

Hoe dit te vertalen naar privacy? De studies naar privacy en surveillance zijn rijke academische onderzoeksgebieden, maar de nadruk ligt vooral op de maatschappelijke, juridische, politieke en technologische aspecten ervan. In tegenstelling tot het klimaat en vervuiling, laten privacy en surveillance zich moeilijk in eenheden uitdrukken. Die op hun beurt weer gebruikt kunnen worden als grens en als stokken om politici en rechters mee te slaan. Daar ligt een interessante uitdaging. Hoe maak je privacy en surveillance meetbaar? Wat is het digitale equivalent van CO_2? En waar ligt de grens?

Praat mee

We zijn nog lang niet uitgepraat over de nieuwe richting van het privacydebat. Op de site van *De Correspondent* discussiëren wij graag verder over de vergelijking tussen privacy en klimaat en manieren waarop privacy als collectief probleem op de kaart kan worden gezet. Praat mee op decorrespondent.nl.

ZELFVERDEDIGINGSGIDS

Zo kun je jezelf (en je omgeving) beschermen

Je kunt ook zelf je digitale data beter beschermen door een aanta eenvoudige maatregelen te nemen op je computer en smartphone. Om je te helpen, hebben we een zelfverdedigingsgids gemaak waarin we heel gerichte aanbevelingen doen voor technologisch hulpmiddelen en een aantal goede gewoonten laten zien voor ho je met je eigen en andermans gegevens om kunt gaan.

Zo leer je stap voor stap je online privacy en veiligheid te ver beteren – én die van je kinderen, vrienden, kennissen en collega's

De gids vind je op **https://corr.es/zelfverdedigingsgids**

Dankwoord

Samen bedanken wij de volgende collega's van *De Correspondent*
Leon Postma, die het omslag heeft ontworpen. *Don't judge a boo*
by its cover, luidt het gezegde. Wel, als de inhoud van dit boek ne
zo fabelachtig beoordeeld wordt als Leons omslagontwerp is, zij
wij tevreden. Floor Milar-Van Sprang en Machteld Vinkenborg
voor hun geweldige hulp bij het verspreiden van de boodschap va
dit boek. Jelmer Mommers, de klimaatexpert van *De Corresponden*
voor de samenwerking voor de epiloog. Onze oud-stagiaires e
onderzoeksassistenten Anne Schepers en Maaike Goslinga, di
ons enorm hebben geholpen bij verschillende onderzoeken. Ernst
Jan Pfauth voor zijn adviezen en ideeën. Rob Wijnberg voor he
bedenken en oprichten van *De Correspondent* waardoor wij al dri
jaar in alle vrijheid de journalistiek kunnen maken die wij belang
rijk vinden. Annelieke Tillema, voor haar secure correctiewer
Andreas Jonkers, die niet alleen de tekst van dit boek strakker hee
getrokken, maar wiens kritische blik en afschrikwekkende gel
rakkers onze artikelen voor *De Correspondent* vanaf het begin a
aan beter hebben gemaakt. Ten slotte: onze uitgever Milou Klei
Lankhorst, voor te veel om op te noemen én voor de dingen di
inderdaad goed zijn gekomen.

Verder zijn wij Ot van Daalen en Jaap-Henk Hoepman bijzo
der dankbaar voor hun kritische en constructieve commentaar o
een eerdere versie van dit boek. Onze grootste dank gaat uit naa
redacteur Harminke Medendorp, die ons tijdens het lange schrij
proces geweldig is blijven begeleiden, óók toen dit boek opeen

heel relatief werd. Door haar prettige bijsturing en advies ligt er nu een boek waar wij enorm trots op zijn.

Ik, Maurits, dank mijn boekenclub. Vanwege de eerste regel van het reglement van de club kan ik helaas niet vertellen waarom. Ik dank al mijn ouders, wier ijskasten, bureaus en – incidenteel – bedden een geweldige basis vormden voor het schrijven van dit boek. Ik dank mijn vrienden, omdat ze mij nog steeds herkennen. Ik dank mijn liefste Renée, de enige persoon voor wie ik niets te verbergen heb. En ten slotte Mia, die er door er eerder te zijn dan verwacht voor zorgde dat dit boek veel later kwam dan gepland, maar die ik geen dag later had willen leren kennen.

Ik, Dimitri, wil mijn kinderen Elias en Nadia en mijn vrouw Nienke bedanken. Weliswaar was hun vader en echtgenoot fysiek aanwezig, maar vaak niet mentaal. Dank voor de bemoedigende knuffels en woorden.

Verantwoording

Veel van de onderzoeken die wij in dit boek beschrijven, hebbe
wij in eerste instantie uitgevoerd voor *De Correspondent*. Sommig
passages in dit boek vertonen daardoor een sterke overlap met o
zijn in sommige gevallen identiek aan passages die al eerder o
De Correspondent verschenen.

Wij beschrijven in dit boek een zoektocht. Daarbij houden we z
veel mogelijk vast aan de chronologische volgorde waarin wij onz
artikelen op *De Correspondent* hebben gepubliceerd. Omwille va
de leesbaarheid en de opbouw van dit boek hebben wij hier ee
enkele keer van afgeweken.

Onze eerste artikelen op *De Correspondent* dateren uit oktober 201
Dit kan als gevolg hebben dat bepaalde informatie die wij toe
vonden nu niet meer precies zo gevonden zou kunnen worden. D
hebben wij voor zover mogelijk gecontroleerd en aangepast. In d
bronnenlijst en op decorrespondent.nl is exact na te zoeken o
welk moment wij de verschillende onderzoeken hebben uitge
voerd en de beschreven informatie hebben gevonden.

Bronnen

Inleiding

1 Dit zei Edward Snowden tijdens een online gesprek op Reddit, in mei 2015. Zie https://www.reddit.com/r/IAmA/comments/36ru89 just_days_left_to_kill_mass_surveillance_under/crglgh2.
2 Eric Schmidt deed deze uitspraak tijdens een interview met CNBC in 2009. Het interview is terug te zien op YouTube via https://www youtube.com/watch?v=A6e7wfDHzew.
3 Maurits Martijn, 'Wanneer data dodelijk kunnen zijn', *De Correspondent* (4 mei 2016). https://decorrespondent.nl/4391/ Wanneer-data-dodelijk-kunnen-zijn/135049596-9c962c25
4 European Commission, *Eurobarometer* (2015). http://ec.europa.eu/ justice/data-protection/files/factsheets/factsheet_data_protection_ eurobarometer_240615_en.pdf
5 Centre for International Governance Innovation & Ipsos, '2016 CGI-Ipsos Global Survey on Internet Security and Trust' (2016). https://www.cigionline.org/internet-survey-2016
6 Smart Health Monitor, een marktonderzoek van Multiscope onder 6.000 Nederlanders (2016). http://www.multiscope.nl/ persberichten/helft-nederlanders-bereid-data-te-delen-met- verzekeraar.html
7 In dit wetenschappelijk paper staat een erg handzaam overzicht va verschillende typen privacy. Bert-Jaap Koops, Bryce Clayton Newel Tjerk Timan, Ivan Škorvánek, Tom Chokrevski en Maša Galič, 'A Typology of Privacy', *University of Pennsylvania Journal of International Law* (24 maart 2016). http://papers.ssrn.com/sol3/ papers.cfm?abstract_id=2754043

1 Smartphones en andere zwarte dozen

8 Bruno Latour, *Pandora's hope: essays on the reality of science studies*, Cambridge, Massachusetts: *Harvard University Press*, 1999.

9 Omer Tene en Jules Polonetsky, *'A Theory of Creepy: Technology, Privacy and Shifting Social Norms'* (2013), *Yale Journal of Law & Technology* (16 september 2013). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2326830

10 De landingspagina van 'What They Know' van *The Wall Street Journal* bevat alle verhalen die in deze serie zijn gemaakt. Je vindt deze pagina via http://www.wsj.com/public/page/what-they-know-digital-privacy.html.

11 De Tracker Tracker-tool is te vinden op de website van het Digital Methods Initiative. https://wiki.digitalmethods.net/Dmi/ToolTrackerTracker

12 'How TV-ads silently ping commands to phones: Sneaky SilverPush code reverse-engineered', *The Register* (20 november 2015). http://www.theregister.co.uk/2015/11/20/silverpush_soundwave_ad_tracker/

13 De verantwoordelijke Amerikaanse toezichthouder FTC heeft appbouwers aangeraden om niet meer met de app, genaamd SilverPush, in zee te gaan.

14 Dat berekende PriceWaterhouseCoopers. Zie http://www.pwc.com/gx/en/industries/entertainment-media/outlook/segment-insights/internet-advertising.html.

15 '2 Billion Consumers Worldwide to Get Smart(phones) by 2016' (2014). http://www.emarketer.com/Article/2-Billion-Consumers-Worldwide-Smartphones-by-2016/1011694

16 Het volledige onderzoek is te lezen op *De Correspondent*. Dimitri Tokmetzis, 'Dit gebeurt er allemaal onder de motorkap van je smartphone' (22 mei 2014). https://decorrespondent.nl/1034/Dit-gebeurt-er-allemaal-onder-de-motorkap-van-je-smartphone/50352698-785491ea

17 'Queen's University, The Globalization of Personal Data Project: An International Survey on Privacy and Surveillance.' (2008)

http://www.sscqueens.org/sites/default/files/2008_Surveillance_Project_International_Survey_Findings_Summary.pdf

18 Helen Nissenbaum, 'A Contextual Approach to Privacy Online' (2011). http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf

19 Dit zei Hal Varian, Googles 'Chief Economist', tegen onderzoeksbureau Pew Research in 2014. Zie: http://www.pewinternet.org/2014/12/18/future-of-privacy/pi_14-12-18_futureprivacy_quotecards_121614_varian/

20 J. Turow, M. Hennesy en N. Draper, 'The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers And Opening Them Up To Exploitation' (2015). https://www.asc.upenn edu/news-events/publications/tradeoff-fallacy-how-marketers-are-misrepresenting-american-consumers-and

2 Hackers en de NSA

21 Bruce Schneier, 'Cyberweapons Have No Allegiance', *Motherboard Vice* (25 februari 2015). https://motherboard.vice.com/read/cyberweapons-have-no-allegiance

22 James Clapper, geciteerd in *The Guardian* op 9 februari 2016. https://www.theguardian.com/technology/2016/feb/09/internet-of-things-smart-home-devices-government-surveillance-james-clapper

23 Maurits Martijn, 'Zo begluur je Nederland vanachter een laptop', *De Correspondent* (13 april 2015). https://decorrespondent.nl/2677/

24 De aflevering 'Zo lek als een mandje' (2014) van *KRO Reporter* bek je hier: http://www.npo.nl/reporter/07-12-2012/KRO_1578525.

25 Maurits Martijn, 'Dit geef je allemaal prijs als je inlogt op een openbaar wifinetwerk', *De Correspondent* (20 maart 2014). https://decorrespondent.nl/845

26 Beelden en uitleg over Newstweek vind je op de projectsite: http://newstweek.com/.

27 Dimitri Tokmetzis, ‘Op deze markt is je creditcard dertien euro waard’, *De Correspondent* (17 februari 2016). https://decorrespondent.nl/3985/Op-deze-markt-is-je-gestolen-creditcard-dertien-euro-waard/194057545-b3ec0c51

28 Het recentste boek van Bruce Schneier is *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton & Company (2015). Veel van zijn werk is terug te vinden op zijn website, https://www.schneier.com/.

29 Dimitri Tokmetzis, ‘In deze virtuele oorlog vechten beide kampen om jouw veiligheid’, *De Correspondent* (23 april 2015). https://decorrespondent.nl/2639/In-deze-virtuele-oorlog-vechten-beide-kampen-om-jouw-veiligheid/128511383-5e1303b3

30 Maaike Goslinga, ‘Een rondje copyshops leert: de grootste vijand van onze privacy zijn we zelf’, *De Correspondent* (14 oktober 2014). https://decorrespondent.nl/1908/Een-rondje-copyshops-leert-de-grootste-vijand-van-onze-privacy-zijn-we-zelf/92913876-36f36bcf

31 Dit cijfer komt uit het onderzoek van Symantec, *State of Privacy Report* (2015). https://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf

32 Dit onderzoek werd uitgevoerd door The Global Commission on Internet Governance voor het rapport *One Internet*, dat hier te downloaden is: https://www.ourinternet.org/report.

3 Google en de Belastingdienst

33 WRR, *iOverheid* (2011). http://www.wrr.nl/publicaties/publicatie/article/ioverheid/

34 Franz Kafka, *Het proces*, 1925.

35 Inspectie Veiligheid en Justitie, *Het overlijden van Alexander Dolmatov* (2013). https://www.ivenj.nl/actueel/inspectierapporten/rapport-het-overlijden-van-alexander-dolmatov.aspx

36 Werkgroep Verkenning kaderwet gegevensuitwisseling, *Kennis delen geeft kracht. Naar een betere en zorgvuldigere gegevensuitwisseling in samenwerkingsverbanden* (2014). https://www.rijksoverheid.nl/documenten/rapporten/2014/12/20/tk-bijlage-verkenning-kaderwet-gegevensuitwisseling

37 WRR, *iOverheid* (2011). http://www.wrr.nl/publicaties/publicatie/article/ioverheid/

38 Het officiële verzoek werd geopenbaard tijdens de rechtszaak die SMSParking had aangespannen. Zie http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBOBR:2013:6553.

39 Maurits Martijn, ‘Vergeet de politiestaat. Welkom in de belastingstaat’, *De Correspondent* (30 september 2014), https://decorrespondent.nl/1766/Vergeet-de-politiestaat-Welkom-in-de-belastingstaat/85998902-f61df5b8

40 Daniel Solove, ‘Privacy and Power: Computer Databases and Metaphors for Information Privacy’, *Stanford Law Review* (juli 2001). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2483

41 Actualiteitenprogramma *EenVandaag* maakte een aantal uitzendingen over Kowsoleea. Zie http://20jaareenvandaag.eenvandaag.nl/hoogtepunten/bestoff/46935/20_jaar_eenvandaag identiteitsfraude_ron_kowsoleea.

42 Voor de uitzending over de digitale doolhof van *De Monitor*, zie http://demonitor.ncrv.nl/digitaal-doolhof.

43 Ibrahim Altaweel, Nathan Good en Chris Hoofnagle, ‘Web Privac Census’, *Technology Science* (15 december 2015). http://papers.ssrn com/sol3/papers.cfm?abstract_id=2703814

44 Dit is een mooi voorbeeld van ‘lock in’; Facebook weet gebruikers en bedrijven binnen te lokken en in een stevige greep te houden.

45 Jennifer Shore en Jill Steinman, ‘Did You Really Agree To That? The Evolution of Facebook’s Privacy’, *Technology Science* (11 augustus 2015). http://techscience.org/a/2015081102/

46 Dat vertelde een analist van Morgan Stanley aan *The New York Times*. Zie http://www.nytimes.com/2016/04/18/business/media-websites-battle-falteringad-revenue-and-traffic.html?_r=4.

47 FTC, *Data Brokers: A Call for Transparency and Accountability* (201 https://www.ftc.gov/system/files/documents/reports/data-broke

call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf

48 Margriet Oostveen, 'Hoe de KNVB en Always meisjes maandverband opdringen', *de Volkskrant* (18 mei 2016). http://www.volkskrant.nl/opinie/hoe-de-knvb-en-always-meisjes-maandverband-opdringen~a4302453/

49 Janet Vertesi, 'My Experiment Opting Out of Big Data Made Me Look Like a Criminal', *Time* (1 mei 2014). http://time.com/83200/privacy-internet-big-data-opt-out/

50 WRR, *Big Data in een vrije en veilige samenleving* (28 april 2016). http://www.wrr.nl/publicaties/publicatie/article/big-data-in-een-vrije-en-veilige-samenleving/

4 Surveillancekapitalisten en sturende overheden

51 Michael Hayden, geciteerd in *The New York Review of Books*, mei 2014. Zie: http://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/

52 Oud-Facebook medewerker Jeffrey Hammerbacher, geciteerd in een artikel van Bloomberg, april 2011. Zie: https://www.bloomberg.com/news/articles/2011-04-14/this-tech-bubble-is-different

53 'Verzamelen metadata geen inbreuk op privacy', *NOS Journaal*. http://nos.nl/video/573000-verzamelen-metadata-geen-inbreuk-op-privacy.html

54 Matt Blaze, 'Phew, NSA Is Just Collecting Metadata (You Should Still Worry)', *Wired* (19 juni 2013). http://www.wired.com/2013/06/phew-it-was-just-metadata-not-think-again/

55 Pedro Cruz Villalón, press release (12 december 2013). http://curia.europa.eu/jcms/upload/docs/application/pdf/2013-12/cp130157en.pdf

56 Op de website van Pentland is meer informatie te vinden over social physics: http://socialphysics.media.mit.edu/.

57 Yves-Alexandre de Montjoye, Laura Radaelli, Vivek Kumar Singh e Alex Pentland, 'Unique in the shopping mall: On the reidentifiability of credit card metadata', *Science* (2015).

58 Meer informatie over het taxionderzoek vind je in Anthony Tocka 'Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset', *Neustar Research* (2014). https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-ny taxicab-dataset/

59 Michal Kosinski et al, 'Private traits and attributes are predictable from digital records of human behavior.' (2013)

60 Anne Schepers, 'De politie van de toekomst houdt iedere burger non-stop in de gaten', *De Correspondent* (7 juli 2015). https://decorrespondent.nl/3044/De-politie-van-de-toekomst-houdt-iedere-burger-non-stop-in-de-gaten/93621264-8dfadf86

61 Een gratis versie van het boek van Rienks is te vinden op de site v de politieacademie. https://www.politieacademie.nl/kennisenonderzoek/kennis/mediatheek/PDF/90696.PDF

62 Een gratis versie van het boek van Sunstein en Thaler is te vinden op de site van Georgetown University. https://ethicslab.georgetow edu/studio/wordpress/wp-content/uploads/2015/02/Richard_H. Thaler_Cass_R._Sunstein_Nudge_Impro_BookFi.org_.pdf

63 Steven de Jong en Floor Rusman, 'Denkt u aan uw aangifte? Dan Liza en Joyce', *NRC Handelsblad* (2 maart 2015). https://www.nrc. nieuws/2015/03/02/denkt-u-aan-uw-aangifte-dank-liza-en-joyce-1473230-a818055

64 James Rule, 'Privacy: the longue durée', *Social Dimensions of Priva* (2015).

65 Het onderzoek van Maurits Kaptein is te vinden op de site van TU Eindhoven via de volgende link: https://pure.tue.nl/ws/files/3470131/729200.pdf.

66 Ashlee Vance, 'This Tech Bubble Is Different', Business Week (14 april 2011). http://www.bloomberg.com/news/articles/2011-04-14/this-tech-bubble-is-different

5 Autonomie en democratie

67 Margriet Overkleeft-Verburg, geciteerd in Maurits Martijn, 'Vergeet de politiestaat. Welkom in de belastingstaat', *De Correspondent* (30 september 2014). https://decorrespondent.nl/1766/Vergeet-de-politiestaat-Welkom-in-de-belastingstaat/85998902-f61df5b8

68 Maxim Februari, 'Hoe we met slimme data de toekomst kwijtraken', *NRC Handelsblad* (10 mei 2016). https://www.nrc.nl/nieuws/2016/05/10/hoe-we-met-slimme-data-de-toekomst-kwijtraken-1616979-a2241956

69 Bart Olmer, ''Terrorist' door verkeerd IP-adres', *de Telegraaf* (12 februari 2015). http://www.telegraaf.nl/binnenland/23674540/___Terrorist__door_IP-adres__.html

70 David Lyon (ed.), *Surveillance as Social Sorting*. Routledge: London, 2003.

71 Meer informatie over social sorting lees je in de bundel van David Lyon die online beschikbaar is via de volgende link. David Lyon (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination* (2003). https://infodocks.files.wordpress.com/2015/01/david_lyon_surveillance_as_social_sorting.pdf

72 Een privacy impact assessment van het ATS-P vind je op de site van het Department of Homeland Security: https://www.dhs.gov/sites/default/files/publications/privacy_pia_cbp_tsacop_09162014.pdf.

73 Voor een goede uitwerking waarom dit het geval is, zie Bart de Koning en Dimitri Tokmetzis, 'Waarom geheime diensten altijd terroristen over het hoofd zullen zien', *De Correspondent* (15 april 2016). https://decorrespondent.nl/4334/Waarom-geheime-diensten-altijd-terroristen-over-het-hoofd-zullen-blijven-zien/211052798-f7fae630

74 Danielle Citron en Frank Pasqualle, 'The Scored Society: Due Process for Automated Predictions', *Washington Law Review* (2014). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2376209

75 Michael Persson, Marije Vlaskamp en Fokke Obbema, 'China kent elke burger een score toe - ook voor internetgedrag', *de Volkskrant* (25 april 2015). http://www.volkskrant.nl/buitenland/china-kent-elke-burger-score-toe-ook-voor-internetgedrag~a3980289/

76 'Apeldoorn voorspelt wie het criminele pad opgaat', *De Stentor* (11 mei 2016). http://www.destentor.nl/regio/apeldoorn/apeldoor voorspelt-wie-het-criminele-pad-opgaat-1.6003931

77 Jeremy Scahill en Ryan Devereaux, 'The Secret Government Rulebook for Labeling You a Terrorist', *The Intercept* (23 juli 2014 https://theintercept.com/2014/07/23/blacklisted/

78 Een toegankelijke lezing waarin Cheney-Lippold zijn ideeën uitwerkt, vind je op YouTube: https://www.youtube.com/watch?v=Qdq4le5hcRU.

79 Julia Angwin, Jeff Larson, Surya Mattu, Laura Kirchner, 'Machine Bias', *ProPublica* (23 mei 2016). https://www.propublica.org/articl machine-bias-risk-assessments-in-criminal-sentencing

80 Anna Maria Barry-Jester, Ben Casselman en Dana Goldstein, 'Should Prison Sentences Be Based On Crimes That Haven't Bee Committed Yet?', *FiveThirtyEight* (4 augustus 2015). http://fivethirtyeight.com/features/prison-reform-risk-assessmen

81 Solon Barocas en Andrew Selbst, 'Big Data's Disparate Impact', *California Law Review* (2016). http://papers.ssrn.com/sol3/papers cfm?abstract_id=2477899

82 Chris Anderson, 'The End of Theory: The Data Deluge Makes th Scientific Method Obsolete', *Wired* (23 juni 2008). http://www.wired.com/2008/06/pb-theory/

83 Rob Wijnberg, 'Hoe onze risicomijdende cultuur de solidariteit ondermijnt', *De Correspondent* (15 juli 2014). https://decorrespondent.nl/1453/Hoe-onze-risicomijdende-cultuur-de-solidariteit-ondermijnt/70756741-e991d6c2

84 Maarten de Rijke en David Graus, 'Wij zijn racisten, daarom Goo ook', *nrc.next* (17 juni 2016). http://www.nrc.nl/nieuws/2016/06/ wij-zijn-racisten-daarom-google-ook-2726583-a1505954

85 Tal Zarsky, 'Mine Your Own Business!: Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion', *Yale Journal of Law and Technology*

(1 januari 2003). http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1008&context=yjolt

86 Charles Duhigg, 'How Companies Learn Your Secrets', New York Times (16 februari 2012). http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

87 Chris Rudder, 'We Experiment on Human Beings!', *OkCupid blog* (28 juli 2014). http://blog.okcupid.com/index.php/we-experiment-on-human-beings/

88 Adam Kramer, Jamie Guillory en Jeffrey Hancock, 'Experimental evidence of massive-scale emotional contagion through social networks', *PNAS* (25 maart 2014). http://www.pnas.org/content/111/24/8788

89 Robert Epstein en Ronald Robbertson, 'The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections', *PNAS* (8 juli 2015). http://www.pnas.org/content/112/33/E4512.abstract

Conclusie: Tijd voor tegenmacht

90 Frank Pasquale, *Black Box Society: The Secret Algorithms That Control Money and Information*. Harvard University Press, 2015.

91 Shoshana Zuboff, 'The New Weapons of Mass Detection', *Frankfurter Allgemeine Zeitung* (13 februari 2014). http://www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/politik-in-der-digitalen-welt/shoshana-zuboff-s-response-to-martin-schulz-the-new-weapons-of-mass-detection-12799987.html?printPagedArticle=true#pageIndex_2

92 Finn Brunton en Helen Nissenbaum, *Obfuscation: A User's Guide for Privacy and Protest*. MIT Press, 2015.

93 We hebben dit voorbeeld ontleend uit het boek *Obfuscation* (2015) van Helen Nissenbaum en Finn Brunton.

94 The Global Commission on Internet Governance, *One Internet* (2016). https://www.ourinternet.org/report

Epiloog: Een nieuw privacyklimaat

95 George Marshall, *Don't Even Think About It: Why Our Brains Are Wired to Ignore Climate Change*. Bloomsbury, 2014.

96 Per Espen Stoknes, *What We Think About When We Try Not To Think About Global Warming*. Chelsea Green, 2015.

Facebook weet bij wie je gisteren op bezoek ging
De Belastingdienst zag hoe je er kwam
Apple hield bij hoelang je er bleef
Samsung hoorde wat je er zei
En Google wist al dat je het van plan was



In *Je hebt wél iets te verbergen* laten onderzoeksjournalisten **Maurits Martijn** (1981) en **Dimitri Tokmetzis** (1975) zien waarom privacy het meest bedreigde mensenrecht van onze tijd is. Ze leggen bloot welke gegevens je allemaal weggeeft en aan wie. En, belangrijker nog: welke ingrijpende gevolgen dat heeft.



Hun journalistieke zoektocht voor *De Correspondent* werd bekroond met diverse prijzen, waaronder De Loep voor de beste online onderzoeksjournalistiek.

“ *Ik heb dit fabelachtige boek met open mond gelezen. Nog nooit werd de discussie rondom privacy zo toegankelijk uitgelegd. Het is van absolute wereldklasse.*

Alexander Klöpping

“ *Dit noodzakelijke boek is een noodklok en strijdershandboek ineen, meeslepend, vloeiend, mobiliserend en informatief geschreven.*

Beatrice de Graaf

“ **VAN ABSOLUTE WERELDKLASSE**
ALEXANDER KLÖPPING

9 789082 520323

Dit boek is een uitgave van *De Correspondent*, een dagelijks medicijn tegen de waan van de dag. Lees de nieuwste artikelen van Maurits Martijn & Dimitri Tokmetzis op **decorrespondent.nl**